Universidad
Carlos III de Madrid
www.uc3m.es

TESIS DOCTORAL

Compliance Framework for Change Management in Cloud Environments

Autor:

Srdan Dzombeta

Directores:

Ricardo Colomo Palacios

Vladimir Stantchev

Tutor:

Juan Miguel Gómez Berbís

DEPARTAMENTO DE INFORMÁTICA

Leganés, Diciembre 2016

Universidad
Carlos III de Madrid
www.uc3m.es

TESIS DOCTORAL

COMPLIANCE FRAMEWORK FOR CHANGE MANAGEMENT IN CLOUD ENVIRONMENTS

Autor: *Srdan Dzombeta*

Directores: Ricardo Colomo Palacios y Vladimir Stantchev

Firma del Tribunal Calificador:

		Firma
Presidente:	Antonio de Amescua Seco	
Vocal:	Ahmed Barnawi	
Secretario:	José Antonio Calvo-Manzano Villalón	

Calificación:

Leganés, de de

I dedicate this dissertation to my parents making my education possible.

It is especially dedicated in memory of my mother. Although she was my inspiration to pursue my doctoral degree, she was unable to see my graduation. This is for her.

RESUMEN

El área de gobernanza, riesgo y cumplimiento (por sus siglas en inglés GRC) es una de las áreas de gestión clave en todas las organizaciones. En el caso de los departamentos de Tecnología de la Información (por sus siglas en inglés IT de *Information Technology*) el área cuenta con una importancia igualmente crucial. Estos departamentos deben orquestar los recursos de capital intelectual y las infraestructuras hardware y software para contribuir a la generación de beneficios empresariales. La literatura ha demostrado que un conjunto de procedimientos en el área GRC es clave para prestar el servicio de forma eficiente a partir del mantenimiento de una infraestructura tecnológica segura y compatible.

Un aspecto importante y particularmente retador en el entorno IT es su constante evolución con el propósito de habilitar la adopción de nuevas tecnologías en apoyo de los procesos corporativos. Dado que la evaluación de riesgos y los aspectos de cumplimiento se refieren a una determinada situación que se puede considerar más o menos estática, los continuos cambios en el entorno IT representan una amenaza para la incorporación de nuevas tecnologías en ámbitos corporativos desde el punto de vista GRC. Por ello, un enfoque sólido para garantizar el cumplimiento no sólo de forma puntual en tiempo y espacio sino de forma integral, considerando el entorno IT en una forma continua e integrada con la gestión del cambio corporativa.

Otro desarrollo importante y modificador de la situación actual es la emergencia de la computación en la nube (CC, siglas en inglés de *Cloud Computing*) como una forma efectiva y eficaz de proporcionar la función IT en las organizaciones. Pese a que CC suscita diversos desafíos para la administración IT, es en particular relevante para GRC ya que habilita la externalización del servicio como una aproximación predominante para proporcionar infraestructura (llamado *Infraestructure-as-a-Service* o IaaS), plataformas (llamado *Platform-as-a-Service* o PaaS) y software (llamado *Software-as-a-Service* o SaaS) dentro de una organización.

CC y la externalización suponen retos más amplios para GRC, ya que implican la inclusión de un proveedor de servicios externo dentro de una organización. Esta circunstancia aflora cuestiones relativas a la selección de proveedores, la gestión de contratos, los acuerdos de nivel de servicio (por sus siglas en inglés SLA), y el seguimiento de las relaciones y los servicios prestados. Estos aspectos, se convierten en un reto aún mayor en el contexto de los cambios frecuentes e interdependientes en el ámbito IT. Por lo tanto, esta tesis está dirigida a la definición y validación de un marco de cumplimiento para la gestión del cambio en entornos relativos a la nube (abreviatura: CFC MCC). La solución propuesta del problema ha sido abordada desde un punto de vista multidisciplinar, tomando en consideración aspectos de la informática, la gestión de IT y el gobierno de IT pero incorporando también aspectos tales como las dimensiones legales y culturales. La solución propuesta proporciona un marco para apoyar la solicitud de requisitos de diferentes áreas (por ejemplo, organizativos, tecnológicos, culturales) y su posterior consideración en el proceso de gestión del cambio de los marcos establecidos de gestión de TI como pueda ser ITIL. EL marco puede ser adaptado a la situación específica de las organizaciones y proporciona un enfoque coherente para abordar los aspectos de GRC en rápida evolución entornos de TI de la organización basados en la nube.

El discurso científico dentro de la tesis se ha estructurado siguiendo las prácticas académicas y recomendaciones de investigación. En la última fase de la metodología de la investigación empírica una validación se ha realizado para verificar la aplicabilidad del marco. Los datos obtenidos de la validación indican que la aplicación del marco para garantizar el cumplimiento en entornos CC constituye una mejora relevante del proceso de gestión del cambio de las organizaciones.

ABSTRACT

The Governance, Risk and Compliance (GRC) area is one of the critical management areas for every organization. This is particularly the case for information technology (IT) departments where both human resources and technical infrastructures (software and hardware) need to work seamlessly in order to provide the expected benefits. The study of the literature shows that sound GRC methods are key to running and maintaining secure and compliant computing infrastructures.

An important and particularly challenging aspect of the IT landscape is its constant and perpetual evolution in order to keep pace with new and emerging technologies that find their way faster and faster into the organizational infrastructure. Since assessments of risks and compliance aspects always refer to a certain (more or less static) situation, such frequent changes pose a real danger to the overall relevance of these assessments in the mid and long-term perspective. So, a sound approach to ensuring compliance not only punctually (both in time and space) but holistically – considering the complete IT landscape in a continuous way – needs to integrate with the change management function of the organization.

Another important development in the last eight to ten years was the emergence of Cloud Computing (CC) as a straightforward and efficient way of providing IT functionality to organizations. While it poses many various challenges to IT management in general, CC is particularly relevant for GRC as it makes an IT provision approach that was previously sometimes applied – outsourcing – to a predominant approach to provide infrastructure (called Infrastructure-as-a-Service or IaaS), platforms (called Platform-as-a-Service or PaaS), and software (called Software-as-a-Service or SaaS) within an organization.

CC and outsourcing entail wider challenges for GRC as it involves the inclusion of an external party as a service provider within an organization reflecting specific aspects of provider selection, contract management, service level agreements (SLAs), and monitoring. They become even more challenging in the context of frequent and interdependent changes. Therefore, this thesis is aimed at the definition and validation of a Compliance Framework for Change Management in Cloud Environments (short: CFC MCC). The proposed solution of the problem has been approached from a multidisciplinary point of view taking in consideration aspects from computer science, IT management and IT governance, but also such aspects as legal and cultural dimensions. The proposed solution provides a framework to support the solicitation of requirements from different subject areas (e.g., organizational, technological, cultural) and their subsequent consideration within the change management process of established IT management frameworks such as ITIL. It can be tailored to the specific situation of most organizations and provides a consistent approach to address GRC aspects in rapidly evolving cloud-based organizational IT landscapes.

The scientific discourse within the thesis has been structured following best academic practices and recommendations. In the last phase of the research methodology an empirical validation has been performed to verify the applicability of the framework. The data obtained from the validation indicate that the application of the framework for ensuring compliance in CC environments constitutes a relevant improvement of the change management process.

TABLE OF CONTENTS

1 Introduction 1

1.1 Significance of the study 2

1.2 Research objectives 3

1.3 Research methodology 5

1.4 Current work and preliminary results 7

1.5 Structure of the thesis 8

2 Background 11

2.1 Change Management in IT 11

2.2 Outsourcing and Cloud Services 14

2.3 Compliance requirements 16

2.4 Frameworks in IT management and governance 18

2.5 Legal Environment for Compliance 19

2.6 Chapter Summary 22

3 Problem formulation and research approach 25

3.1 Research Problem 25

3.2 Research Approach 26

3.3 Limitations on validity 28

4 Compliance Framework for Change Management in Cloud Environments 31

4.1 Overview of the Framework 32

4.2 Motivation 33

4.3 Qualitative Studies using the Nominal Group Technique 37

4.4 Legal Environment 38

4.5 Organizational and processual environments 47

4.6 Technological Environment 53

4.7 Cultural Environment 59

4.8 The Inner Works 64

4.9 Summary of the Framework 78

5 Validation of the framework by experts 81

5.1 Validation Approach 81

5.2 Validation of the items of the framework 82

5.3 Validation of the framework as a whole 96

6 Adaptation of the Framework after Validation 99

6.1 Legal Area ... 99

6.2 Organizational and Processual Area ... 101

6.3 Technological Area ... 103

6.4 Cultural Area ... 105

6.5 Summary of Framework Adaptation ... 107

7 Evaluation ... 108

7.1 Evaluation Approach ... 108

7.2 Evaluation Plan ... 110

7.3 Evaluation Execution ... 112

7.4 Analysis ... 117

7.5 Revisiting the research questions and hypotheses ... 163

7.6 Discussion of Results ... 164

8 Conclusion and Outlook ... 169

8.1 Accomplishment of Objectives ... 170

8.2 Main contributions ... 171

8.3 Benefits of the Proposed Framework ... 171

8.4 Critical Reflection and Lessons Learned ... 172

8.5 Potentials for Future Applications and Further Development of the Framework ... 173

8.6 Outlook on Future Research Activities in the Area ... 173

9 References ... 175

LIST OF FIGURES

Figure 1. An overview of the proposed research approach 27
Figure 2. A schematic overview of the proposed framework 32
Figure 3. Applied laws for Cloud Data depending on the host country 39
Figure 4. Overview of Layers in Cloud Computing and the Cloud Services provided at each level 47
Figure 5. General overview of Shelp & Stutz's SOA-Governance-Model 49
Figure 6. The Henderson and Venkatraman Strategic Alignment Model 50
Figure 7. Wheeler's E-Business Innovation cycle 55
Figure 8. Technology Acceptance Model (TAM) 56
Figure 9. A Standard Change Management Process in ITIL V3 67
Figure 10. An Architectural Overview of the Inner Works of CFC MCC 69
Figure 11. Documentation of Suggested Clarification in LEGAL area (in German) 85
Figure 12. Documentation of Suggested Frequency (W) and Frequency (H) of Triggers from Expert 1 86
Figure 13. Documentation of Suggested Frequency (left) and Frequency (right) of Triggers from Expert 2 87
Figure 14. Summary of Assessment all Questions – left column (ok), middle column (to be removed), right column (to be added) 88
Figure 15. A View of the MS SharePoint Portal that was used during Framework Customization with Evaluation Partner 1 116
Figure 16. Distribution of roles among the sample in Phase 1 Case Study 1 118
Figure 17. Satisfaction Compliance Management in CC. Phase 1 of Case Study 1 119
Figure 18. Satisfaction on CC Service. Phase 1 of Case Study 1 119
Figure 19. Contribution of compliance management in CC to IT quality of service. Phase 1 of Case Study 1 120
Figure 20. Contribution of compliance management in CC to corporate compliance management. Phase 1 of Case Study 1 121
Figure 21. Distribution of roles among the sample in Phase 1 of Case Study 2 125
Figure 22. Satisfaction Compliance Management in CC. Phase 1 of Case Study 2 126
Figure 23. Satisfaction on CC Service. Phase 1 of Case Study 2 127
Figure 24. Contribution of compliance management in CC to IT quality of service. Phase 1 of Case Study 2 128
Figure 25. Contribution of compliance management in CC to corporate compliance management. Phase 1 of Case Study 2 128
Figure 26. Satisfaction Compliance Management in CC. Phase 2 of Case Study 1 135
Figure 27. Satisfaction on CC Service. Phase 2 of Case Study 1 136
Figure 28. Contribution of compliance management in CC to IT quality of service. Phase 2 of Case Study 1 136
Figure 29. Contribution of compliance management in CC to corporate compliance management. Phase 2 of Case Study 1 137
Figure 30. Satisfaction Compliance Management in CC. Phase 2 Case Study 2 143
Figure 31. Satisfaction on CC Service. Phase 2 Case Study 2 144
Figure 32. Contribution of compliance management in CC to IT quality of service. Phase 2 Case Study 2 144

Figure 33. Contribution of compliance management in CC to corporate compliance management. Phase 2 Case Study 2 145
Figure 34. A Visualization of Improvement in Maturity Levels before (blue) and after (red) Framework introduction at Evaluation Partner 2 / Case Study 2 154

LIST OF TABLES

Table 1. Consideration of the Proposed Subject Areas (legal, organizational /processual, technological, cultural) in Relevant Standards ... 34
Table 2. The proposed Questionnaire for soliciting Input from Legal Environment ... 45
Table 3. The proposed Questionnaire for soliciting Input from Organizational and Processual Environment ... 51
Table 4. The proposed Questionnaire for soliciting Input from Technological Environment ... 57
Table 5. The proposed Questionnaire for soliciting Input from Cultural Environment ... 63
Table 6. Proposed Protection Requirements Categories ... 70
Table 7. Decision Support for Defining Requirements Categories per Topic Area ... 71
Table 8. Example for Defining Requirements Categories per Topic Area ... 74
Table 9. A Risk Matrix as an Example for Documentation of Gross Risk (ToS – Threshold of Significance) ... 75
Table 10. Example for Documenting Existing Control Measures per Topic Area ... 75
Table 11. Example for Documenting Gross Risk ... 77
Table 12. Example for Defining Measures for Change Management in CC ... 77
Table 13. Improved Version of Questionnaire for Legal Environment after Validation ... 100
Table 14. Improved Version of Questionnaire for Organizational and Processual Environment after Validation ... 102
Table 15. Improved Version of Questionnaire for Technological Environment after Validation ... 104
Table 16. Improved Version of Questionnaire for Cultural Environment after Validation ... 106
Table 17. Compliance evaluation sheet. Phase 1 of Case Study 1 ... 121
Table 18. ANOVA results among roles. Phase 1 of Case Study 1 ... 122
Table 19. Student T test results between CIO and Manager. Phase 1 of Case Study 1 ... 122
Table 20. Student T test results between CIO and Group Leaders. Phase 1 of Case Study 1 ... 123
Table 21. Student T test results between Managers and Group Leaders. Phase 1 of Case Study 1 ... 123
Table 22. Main Compliance Metrics. Phase 1 of Case Study 1 ... 124
Table 23. Answered Questions related to Maturity Level 2 before Framework Introduction (in German) ... 124
Table 24. Compliance evaluation sheet. Phase 1 of Case Study 2 ... 128
Table 25. ANOVA results among roles. Phase 1 of Case Study 2 ... 129
Table 26. Student T test results between CIOs and Managers. Phase 1 of Case Study 2 ... 130
Table 27. Student T test results between CIO and Group Leaders. Phase 1 of Case Study 2 ... 130
Table 28. Student T test results between Managers and Group Leaders. Phase 1 of Case Study 2 ... 131
Table 29. Main Compliance Metrics. Phase 1 of Case Study 2 ... 131
Table 30. Question Areas and their Maturity Levels before Framework Introduction at Partner 2 / Case Study 2 ... 132
Table 31. Descriptive statistics on compliance evaluation sheet. Phase 1, overall comparison ... 132
Table 32. Student T test results between case studies. Phase 1, overall comparison ... 133
Table 33. Compliance Metrics, Phase 1, overall comparison ... 133
Table 34. Compliance evaluation sheet. Phase 2 of Case Study 1 ... 137
Table 35. ANOVA results among roles. Phase 2 of Case Study 1 ... 138

Table 36. Student T test results between CIO and Managers. Phase 2 of Case Study 1 138
Table 37. Student T test results between CIO and Group Leaders. Phase 2 of Case Study 1 ... 139
Table 38. Student T test results between Managers and Group Leaders. Phase 2 of Case Study 1 139
Table 39. Main Compliance Metrics. Phase 2 of Case Study 1 139
Table 40. Answered Questions related to Maturity Level 2 after Framework Introduction (in German) 140
Table 41. Answered Questions related to Maturity Level 3 after Framework Introduction (in German) 141
Table 42. Compliance evaluation sheet. Phase 2 of Case Study 2 145
Table 43. ANOVA results among roles. Phase 2 of Case Study 2 146
Table 44. Student T test results between CIOs and Managers. Phase 2 of Case Study 2 146
Table 45. Student T test results between CIOs and Group Leaders. Phase 2 of Case Study 2. 147
Table 46. Student T test results between Managers and Group Leaders. Phase 2 of Case Study 2 147
Table 47. Main Compliance Metrics. Phase 2 Case Study 2 148
Table 48. Questions related to different Maturity Levels (ML, column 1) and Answers (yes/no) per Areas after Framework Introduction at Partner 2 / Case Study 2 148
Table 49. Maturity Levels per Areas before (Column 2) and after (Column 3) Framework Introduction at Partner 2 / Case Study 2 153
Table 50. Descriptive statistics on compliance evaluation sheet. Phase 2, overall comparison 155
Table 51. Student T test results between case studies. Phase 2, overall comparison 155
Table 52. Compliance Metrics, Phase 2, overall comparison 156
Table 53. Descriptive statistics on compliance evaluation sheet. Phase 3 Case Study 1 157
Table 54. Student T test results between Phases. Case Study 1 158
Table 55. Compliance Metrics, Comparison of Phases. Case Study 1 158
Table 56. Descriptive statistics on compliance evaluation sheet. Phase 3 Case Study 2 159
Table 57. Student T test results between Phases. Case Study 2 160
Table 58. Compliance Metrics, Comparison of Phases. Case Study 2 160
Table 59. Descriptive statistics on compliance evaluation sheet. Phase 3, overall comparison 162
Table 60. Student T test results between case studies. Phase 3, overall comparison 162
Table 61. Compliance Metrics, Phase 3, overall comparison 163

1 Introduction

Cloud computing (CC) is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. (Mell & Grance, 2011). CC is technology that evolved from distributed, grid, and utility computing (Shiau & Chau, 2016) and now has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Nowadays, cloud computing has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased (Armbrust et al., 2010). The cloud offers several benefits like fast deployment, pay-for-use, lower costs, scalability, rapid provisioning, rapid elasticity, ubiquitous network access, greater resiliency, hypervisor protection against network attacks, low-cost disaster recovery and data storage solutions, on-demand security controls, real time detection of system tampering and rapid re-constitution of services (Subashini & Kavitha, 2011). According to Gartner (2016), by 2019, more than 30 percent of the 100 largest vendors' new software investments will have shifted from cloud-first to cloud-only According to Stratistics MRC (2016), the Global Cloud Computing Market is accounted for $103.35 billion in 2015 and is poised to reach $512.81 billion by 2022 growing 25.7% yearly during the forecast period. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is (Popović & Hocenski, 2010). More recently security, trust and privacy remain challenges for organizations that adopt CC (Chang, Kuo, & Ramachandran, 2016; Chang & Ramachandran, 2016),

Once in CC, IT systems, processes or procedures, have to fulfill various compliance requirements. Compliance requirements are typically associated with regulations that may be introduced externally or internally for an organization itself (Abdullah, Indulska, & Sadiq, 2016). These requirements may stem from different sources: legislature and regulatory bodies standards and codes of practice, organizational policies and business partner contracts. However, in many cases these are not fully or not in time identified or even not properly implemented. This usually leads to additional costs, delays and increased liability risks in the project or operation phase. Information Technology compliance is one of the hottest issues in IT and technology management fields (Kim, 2007). The term Compliance means adherence to all legal duties, regulations and guidelines relevant to a company. According to Kim (2007), IT compliance means an accordance of corporate IT systems with predefined policies, procedures, standards, guidelines, specifications, or legislation. In this new scenario, the usage of cloud services for data and information implies additional complexity regarding these compliance requirements and risks. In CC changes have to be tracked across different platforms and involved parties, for example, various processes, applications, and hosting providers (Koetter, Kochanowski, Renner, Fehling, & Leymann, 2013). Because of the very nature of cloud technology, compliance is a shared responsibility among organizations and service providers; it involves service providers, service brokers, customers, and auditors (Yimam & Fernandez, 2016).

In this changing environment in which risks are usually before the project starts, many of the problems are rooted in uncontrolled changes during the project or operating phase. The cost of not being compliant may result in penalty fees, lawsuits, and bad business reputation (Yimam & Fernandez, 2016).

In CC settings, relevant technical and organizational measures, key performance indicators or essential processes like the change management process are often not adequately defined (Akande, April, & Van Belle, 2013). In general, these risks are due to missing, insufficient or untimely integration of important functions such as compliance officers, IT security officers or privacy officers. But more important, in this context there is a need to count on defined management processes like contract, demand or change management. These organizational structures and processes form the pillars of a compliance framework which is the essential success factor for outsourcing projects especially into the cloud.

In this doctoral thesis, it is aimed to analyse and assess existing compliance requirements with respect to the areas of information security and data protection in the context of CC. This assessment considers both the industrial view and the state-of-the-art research within the scientific community. To do so, a framework for the assertion of compliance is proposed. It incorporates compliance assessment as part of the organizational change management process and thus provides a clearly specified approach for dealing with compliance requirements in the context of changes in a cloud-enabled organization.

1.1 Significance of the study

IT-Governance is considered a main objective of the information management function (Meyer, Zarnekow, & Kolbe, 2003) and imperative for business organizations to meet the challenges presented by the business environment (Alreemy, Chang, Walters, & Wills, 2016). As a result of its importance, it is a fertile area of research in the information systems arena since the early 2000s (Grembergen, 2003; Juiz & Toomey, 2015; Van Grembergen & De Haes, 2009).

The importance of IT governance for the enterprise increased correspondingly to the added value that IT was providing (Bin-Abbas & Bakry, 2014; Buchwald, Urbach, & Ahlemann, 2014; Tsai, Chou, Leu, Chen, & Tsaur, 2015) and was put further into focus by the introduction of regulatory mechanisms such as the Sarbanes-Oxley-Act (Damianides, 2005; Karanja & Zaveri, 2014).

The governance of cloud-computing scenarios is considered a part of the overall IT-Governance objective (Petruch, Stantchev, & Tamm, 2011) and mitigate inherent risks in the CC area (Sesay & Ramirez, 2016). Research in the area has developed considerably during the last years and various approaches for the governance of CC have been proposed (Hsu, 2012; Joha & Janssen, 2012; Prasad & Green, 2015), as the works of (Becker & Bailey, 2014) point out.

CC itself is considered a disruptive and transformative technology (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011) that will greatly enhance the added value of IT while providing the organization with increased flexibility to adapt to changing market environments – both resource-wise and with respect to functionality enhancements. On the other side, there exist major concerns regarding data protection, information security, availability and other relevant aspects of a cloud service depending on delivery models (Subashini & Kavitha, 2011) or governance aspects (Petruch et al., 2011).

In this scenario, Change Management is seen as a way to approach the problem combining business perspectives and impact assessment. Change management has been defined as 'the process of continually renewing an organization's direction, structure, and capabilities to serve the ever-changing needs of external and internal customers (Moran & Brightman, 2000). Moreover, a successful management of change is crucial to any organization in order to survive and succeed in the present highly competitive and continuously evolving business environment (By, 2005). In CC settings, change management has been pointed out as an approach to solve some of the issues on its adoption and further development in several aspects (Martens & Teuteberg, 2012; Owens, 2010; Sultan, 2013). Taking this into account, the aim of this doctoral thesis is the integration of the governance aspects of CC decisions into the change management process of an organization. The main hypothesis is that this integration will provide an approach beneficial for the organizations that apply it.

1.2 Research objectives

The objective of this doctoral thesis is the definition of a compliance framework suited to outsourcing projects and the operating phase in a cloud service environment. This framework will include a method for developing, evaluating and analyzing requirements and defining required measures and controlled procedures. The main focus will be on the change management process during the project and operation phase. The compliance framework will help to improve changes, reduces the risks and fulfill almost all legal requirements. The results of the function of the framework will be statistically analyzed. For this purpose, an extensive questionnaire will be defined and results of participating companies will be evaluated.

This doctoral thesis focuses on the design of a comprehensive framework based on the approach presented herein, and with the capabilities of addressing the proposed research challenges. Thus, the research objectives can be broken down into the following sub-objectives:

Objective 1. Investigate and gather existing models, constructs and approaches within the industry and the research community related to the aims of this work.

Objective 2. Collect, unify and improve existing approaches if any, and propose new techniques and standards if required to solve the described problem.

Objective 3. Devise and design an approach, based on study previously performed, and with the capabilities for meeting the research challenges pointed out in this document.

Objective 4. Develop a framework as an artifact that permits its evaluation in terms of applicability, quality efficiency, and efficacy aimed to demonstrate its feasibility to solve the business problem.

Objective 5. Validate the framework in real-world scenarios.

Objective 6. Evaluate the proposed framework and compare it with related research contributions in the area and other existing approaches in the industry if any.

1.2.1 Research Question

The outcomes of this doctoral work are focused on the development of a compliance framework to address the proposed research challenges aforementioned. Consequently, under these premises, it arises the research question about the existence of appropriate compliance framework to support organizations in compliance issues in CC environments.

1.2.2 Hypothesis

Taking into consideration what stated above, it is possible to formulate the hypothesis aimed to be validated in this doctoral thesis, as follows:

> ***If*** *there exists a framework that allows corporations to fulfil compliance needs in CC setting, in a timely manner, and regardless of their systems and compliance requirements,* ***then*** *such framework can be adopted by organizations to manage and optimize their business performance.*

1.3 Research methodology

The proposed research method for this thesis will follow the design-science paradigm for Information Systems research. More specifically, the Information Systems Research Framework described in (Hevner, March, Park, & Ram, 2004) and (Chatterjee, 2010) will be extended and adapted for the purpose of this work. According to it, the fundamental principle of design-science research is that "knowledge and understanding of a design problem and its solution are acquired in the building and application of an artifact".

This work will follow the seven foundational guidelines of the framework (Chatterjee, 2010) as follows:

Guideline 1: Design as an artifact.

"Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation".

The author proposes to build a framework that ensures compliance for cloud-computing services as part of the organizational change management.

Guideline 2: Problem relevance.

"The objective of design-science research is to develop technology-based solutions to important and relevant business problems".

The construction of the proposed framework will provide organizations with the ability to assess governance and compliance aspects of CC offerings as part of the change management process. This will allow the organization to ensure compliance for its cloud-based services from the onset and thus will minimize operation of non-compliant services by or for the organization Furthermore, organizations will be able to explore CC more aggressively, as the primarily concerns about the adoption of cloud services – security and non-compliance – are addressed in a consistent way.

Guideline 3: Design evaluation.

"The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods".

The design evaluation approach used in this thesis encompasses an empirical research methodology. More specifically, key aspects of the proposed framework will first be verified by expert interviews, then by experimental settings in specific organizations. Results will be evaluated qualitatively and also quantitatively (where the data basis allows it). Examples of quantitative assessments can be the changes in specific key performance indicators (KPIs) in the organization.

Guideline 4: Research contributions.

“Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies”.

The proposed compliance framework is novel and it will address the specific intersection of (a) governance and compliance, (b) cloud computing, and (c) change management.

The main research contributions are focused on filling the gaps between these three areas and thereby providing a generally applicable framework that is domain-independent and technology-agnostic. Another research contribution will be the suggestion of specific blueprints that are relevant for specific sectors with healthcare being a possible example.

Guideline 5: Research rigor.

“Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact”.

The proposed framework will be developed after a structured and in-depth assessment of related works in the research landscape. Each important construct of the framework will be rigorously evaluated with respect to its contribution to the overall framework aims while both framework and individual constructs will be considered through the prism of whether they verify or falsify to posited hypotheses.

Guideline 6: Design as a search process.

“The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment”.

The artifact design will be undertaken incrementally and iteratively by refining the framework and the underlying assumptions against new research challenges, alternatives or issues.

Guideline 7: Communication of research.

“Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences”.

This work is intended to be distributed on a diverse set of scientific journals, international conferences and book chapters, as well as published by the *Universidad Carlos III de Madrid* in partial fulfilment of the requirements for the Ph.D. program in “*Ciencia y Tecnología Informática*”.

1.4 Current work and preliminary results

Currently, there exist different approaches and disaggregated techniques in the research community that aim to address the problem mentioned above. However, these are typically constrained to a specific subset (e.g. legal or technical) and hardly applicable. This is in part due to the specific viewpoints of IT governance and compliance (Simonsson, Johnson, & Ekstedt, 2010), as compared to the ones of cloud adoption (Kim, 2011) and change management (By, 2005). Thus, they are not sufficient to meet consistently the research objectives of this work.

This thesis is based on the decade-long experience of the author in the definition and development of Information Security Management Systems (ISMS), as well as in the assessment of such systems during compliance audits. The proposed framework will serve as a model for future activities in these fields, once it has been developed and evaluated.

A first top-level version of the framework has been developed, based on an extensive analysis of the state-of-the-art research in the area. Furthermore, the input fields of the framework have been elaborated. Currently, the author is developing further the inner workings of the framework and the proposed evaluation approaches.

Some preliminary results have already been presented in the following publications:

- Haufe, K., Dzombeta, S., Brandis, K., Stantchev, V., & Colomo-Palacios, R. (n.a). **Improving transparency and efficiency in IT security management resourcing. IEEE IT Professional**, in press (Impact factor 2015: 1.067; COMPUTER SCIENCE, SOFTWARE ENGINEERING, 47/106, Q2)
- Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). **ISMS core processes: A study**. In Proceedings of CENTERIS 2016 - Conference on ENTERprise Information Systems / ProjMAN 2016, Procedia Technology, Volume 100, 2016, pp. 339-346, Porto, Portugal, October 5-7. http://dx.doi.org/10.1016/j.procs.2016.09.167
- Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). **Security Management Standards: A Mapping**. In Proceedings of CENTERIS 2016 - Conference on ENTERprise Information Systems / ProjMAN 2016, Procedia Technology, Volume 100, 2016, pp. 755-761, Porto, Portugal, October 5-7. http://dx.doi.org/10.1016/j.procs.2016.09.221
- Dzombeta, S., Stantchev, V., Colomo-Palacios, R., Brandis, K., & Haufe, K. (2014). **Governance of cloud computing services for the life sciences – the case of Germany in the context of EU**. IEEE IT Professional, 16(4), 30-37. (Impact factor 2014: 0.819; COMPUTER SCIENCE, INFORMATION SYSTEMS, 62/104, Q3) http://dx.doi.org/10.1109/MITP.2014.52
- Haufe, K., Dzombeta, S., & Brandis, K. (2014). **Proposal for a security management in cloud computing for health care**. The Scientific World Journal, 2014, Article ID 146970. http://dx.doi.org/10.1155/2014/146970

- Brandis, K., Dzombeta, S., & Haufe, K. (2013). **Towards a framework for governance architecture management in cloud environments: A semantic perspective**. *Future Generation Computer Systems*. 32 (2014): 274-281 (Impact factor 2014: 2.786; COMPUTER SCIENCE, THEORY & METHODS, 8/102, Q1) http://dx.doi.org/10.1016/j.future.2013.09.022
- Stantchev, V., Dzombeta, S., Brandis, K., Colomo-Palacios, R. (2013). **Proposal for a compliance framework for change management in cloud environments.** *In proceedings of the 6th World Summit on the Knowledge Society, Aveiro, Portugal, 19-21 June 2013.*
- Arendt, B., Dzombeta, S. (2013). **Outsourcing im Gesundheitswesen**. Privacy in Gesundheitswesen 01.13, pp. 39-44 (in German)
- Dzombeta, S., Goldstein, O. (2013) **Patientendaten und Cloud Computing**, BITKOM Whitepaper, available online at: http://www.digitalewelt.org/content/wie-geht-es-weiter-mit-der-cloud

1.5 Structure of the thesis

The subject of this thesis is a Compliance Framework for Change Management in Cloud Environments (CFC MCC). The thesis is divided in eight main sections which are: introduction, state of the art research, research objectives and approach, main contribution (the framework), validation, adaptation, evaluation, and conclusion. It starts with an introduction of the topic field that also includes an assessment of the significance of the problem, and a description of the chosen research methodology. The background reviews the state-of-the-art research in relevant areas such as change management, outsourcing and CC, compliance requirements and their legal environment. Then, the research objectives are specified and the approach is outlined. An elaboration of the developed framework follows that covers both the architectural level and the detail level. Subsequently, the conducted validation is described. The validation provided important expert opinions about the improvement and adaptation of the framework which followed. Then, the evaluation of the framework is presented, together with its objectives, conduction and results. Finally, the conclusion of the work and the outlook on future research activities in the area are given.

Chapter 1. Introduction. The introduction discusses the emergence of cloud computing, as well as the governance, risk and compliance challenges associated with it. The significance of the problem is derived from the importance of IT governance and the relevance of change management for maintaining a performant and compliant IT infrastructure. The research method applied for this thesis follows the design-science paradigm for Information Systems research.

Chapter 2. Background. In the background an analysis of the state of the art research in the relevant sub-domains is given. Specifically, the areas of change management, outsourcing and cloud services, compliance requirements, frameworks and their success factors, and legal environment for compliance are assessed, discussed and structured.

Chapter 3. Research Objectives and Approach. This chapter gives the operationalisation of the overall thesis objective into specific, measurable and concrete objectives that serve as directions for the next phases of the thesis. It also introduces the approach of thesis conduction.

Chapter 4. Compliance Framework for Change Management in Cloud Environments. This chapter introduces the main contribution of the thesis – the framework. After a motivation about the necessity of it, the framework is described together with its overall structure, its different subject areas, its lifecycle-based approach, and its integration into traditional change management environments.

Chapter 5. Validation of Framework Items. The framework was subjected to an extensive expert validation after it has been developed. This chapter describes the conduction of the expert workshops and the results that were derived by them.

Chapter 6. Adaptation of the Framework after First Validation. This chapter describes the adaptations of the framework that were introduced to incorporate and reflect experts' feedback from the validation phase.

Chapter 7. Evaluation. This chapter documents the evaluation of the framework. It includes a discussion of the evaluation objectives, the concept of the evaluation, the requirements on potential organizations where the evaluation can be conducted, the selection process, the actual conduction of the evaluation, the obtained evaluation results, and their discussion.

Chapter 8. Conclusion and Outlook. In this final chapter, the results and the benefits provided by the research work are analysed and assessed in light of current developments. The potentials for future applications and further development of the framework are also discussed. The chapter also provides an outlook on future research activities in the area.

2 Background

This chapter starts with the landscape of change management section. Further, it continues with surveying outsourcing and cloud services in detail. After having introduced the notion of compliance requirements and their repercussion in the literature, the next part is devoted to study and present the main frameworks and its success in the field of IT management. The last part of this chapter concludes with an overview of the legal environment for compliance, particularly in the field of CC.

2.1 Change Management in IT

Each organization is based on at least one process – the basic "sequence of tasks" that entails its primarily purpose (Frick, 2012). A business process – a specific type of the process – is always based on the added value of a service that is offered to a customer (Tiemeyer, 2009). The successful management of change is crucial for every organization (By, 2005) and change management has been defined as "the process of continually renewing an organization's direction, structure, and capabilities to serve the ever-changing needs of external and internal customers" (Moran & Brightman, 2001). Types of change that arise for an organization can be classified according to several criteria consistent with a meta-analysis conducted in 2005 (By, 2005):

- Their rate of occurrence: discontinuous, incremental, smooth incremental, bumpy incremental, continuous, continuous incremental, and punctuated equilibrium with discontinuous and incremental considered main types;
- How it comes about: planned, emergent, contingency, and choice;
- By scale: fine-tuning (or convergent change), incremental adjustment, modular transformation, and corporate transformation.

The change management process in general can encompass the following phases (Gama, Nunes da Silva, & Mira da Silva, 2011; Van Bon, 2008):

- identification, registration, and acceptance of change requests;
- classification;
- approval (e.g., by a Change Advisory Board - CAB);
- implementation;
- control (often called post implementation review – PIR).

Within the first step a formal request for change (RFC) is submitted. After its acceptance the RFC is classified (e.g., according to importance, impact) and then comes the approval phase. The implementation phase differs widely with respect to subject matter, effort, duration. The control phase assures that the implementation was conducted accordingly and that the introduced change is meeting the expectations.

Most of the literature argues that the use of change management practices has a positive effect on the speed and quality of the change process and on results for the organization (Yamakawa, Obregón-Noriega, Novoa Linares, & Vega Ramírez, 2012). In the IT service scenario, according to Galup, Dattero, Quan and Conger (2009), establishing a set of uniform processes (such as Incident Management, Change Management, etc.) enables the delivery of IT services consistently within a single. Moreover, change management is considered critical for ITIL implementations (Pollard & Cater-Steel, 2009). Other literature e.g. (Lema, Calvo-Manzano, Colomo-Palacios, & Arcilla, 2015; Tan, Cater-Steel, & Toleman, 2009) consider change management as a critical success factor in ITIL. Information Technology Infrastructure Library (ITIL) is a standard of best practices whose objective is to manage ICT infrastructure efficiently, with the objective of guaranteeing the levels of service agreed upon by the ICT organization and its clients (Van Bon et al., 2010). ITIL in version 3 consists of a set of five books published by the Office of Government Commerce (OGC), which empowers an ICT organization to improve the service it offers to its clients. Each of the books covers a specific area: Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement; this set has been entitled ITIL Core. For each area, ITIL defines objectives, activities, and the inputs and outputs of the processes of the organization (Casado-Lumbreras, Colomo-Palacios, Hernández-López, & Soto-Acosta, 2011). ITIL process are: Incident Management, Problem Management, Release Management, Change Management, Configuration Management, Service Level Management, Financial Management of IT Services, Capacity Management, IT Service Continuity Management, and Availability Management (McNaughton, Ray, & Lewis, 2010). In the ITIL world, IT service change management aims to ensure that new services and changes to services will be deliverable and manageable at the agreed cost and service quality (Jäntti & Hotti, 2016).

This definition lead us to other perspective on change management in the IT arena: IT Governance. Service management includes the management of the process (Krallmann, Schröpfer, Stantchev, & Offermann, 2008) which includes its governance and control (Petruch et al., 2011). A well-managed organization applies a management system that includes all of its relevant processes – both core and supporting – as there is potential for improvement in both areas. Information technology governance is the structure that permits compatibility among the strategic goals of the corporation and the intentions that will aid the corporation realise a satisfactory stage of risk (Alreemy et al., 2016). "Governance of IT", that has its origins in corporate governance, is equivalent to "corporate governance of IT," "enterprise governance of IT," and "organizational governance of IT" (Juiz & Toomey, 2015). ISO/IEC 38500 published in 2008 is the first international standard to provide guidelines for governance of IT. ISO/IEC 38500 defines a Governance, Risk and Compliance Model that regulates the intra technological support of business processes, evaluating and controlling them (Michelberger Jr & Lábodi, 2012). ISO/IEC 38500 draws six principles:

1. responsibility to address individuals and groups within the organization, understand and accept their responsibilities with respect to both the supply of, and demand for IT;
2. strategy to take into account the current and future IT capabilities;
3. acquisition to acquire requirements made for valid reasons, based on an appropriate and ongoing analysis;
4. performance to analyse and decide appropriate levels and quality of service necessary to meet current and future business requirements;
5. conformance to track policies and practices clearly defined, implemented and enforced;
6. human behaviour to observe policies, practices and decisions demonstrations with respect to human behaviour.

Although change management is pervasive in the initiative, according to Wilkin and Campbell (2010), change management is particularly important for the fifth principle: Conformance, since Change management must be established to facilitate achievement of benefits.

The importance of IT Governance in general and ISO/IEC 38500 has been recognized widely in the literature e.g. (Chou & Liao, 2015; De Haes, Huygh, Joshi, & Van Grembergen, 2016; Lombardi, Giudice, Caputo, Evangelista, & Russo, 2015; Schlosser, Beimborn, Weitzel, & Wagner, 2015; Sesay & Ramirez, 2016; Tiwana & Kim, 2015; Tsai et al., 2015; Wilkin, Campbell, & Moore, 2013) and the integration of IT Governance principles in the final framework is key in the creation of a sound and grounded research approach.

The next initiative to review is Capability Maturity Model Integration for Services (CMMi-SVC). CMMi-SVC is a maturity model which covers the activities necessary to manage, establish and deliver services (CMMI Product Team, 2010). Similarly to its twin models it was created by the Software Engineering Institute (SEI) with the intention of defining constellations for being applied in different areas of interest. CMMi-SVR contains elements in common with CMMi-DEV and CMMi-ACQ, and adds objectives and practices specific to the provision of services. CMMI-SVC best practices focus on activities for providing quality services to the customer and end users (Mesquida, Mas, Amengual, & Calvo-Manzano, 2012). Again, Change Management is a widespread procedure supporting generic goals and practices like Training but also support process areas like Configuration Management. Again, and like all the previous cases, literature has recognized the importance of the initiative in a set of recent and relevant works e.g. (Kalinowski, Biffl, Spínola, & Reinehr, 2014; Kundu & Manohar, 2012; Mora, Raisinghani, O'Connor, Marx-Gomez, & Gelman, 2014; O'Connor, Raisinghani, Mora, Marx-Gomez, & Gelman, 2015).

Finally, in the scientific community there exist some application or technology-specific change management approaches, e.g., for ERP systems (Aladwani, 2001), or in the context of business process reengineering (Earl, Sampler, & Short, 1995; Grover, Jeong, Kettinger, & Teng, 1995). In general, they follow a similar approach, often with a more simplified view, e.g., 3 phases in (Aladwani, 2001).

To sum up, several initiatives consider change management a key issue for IT Service Management and this process is, taking into account the literature review conducted, part of the most important initiatives in the field. However, the connection of change management with compliance management has not been analyzed in deep by researchers.

2.2 Outsourcing and Cloud Services

CC can be seen as a paradigm change in the evolution of computing. In an era of ubiquitous networking, CC responds to the needs of the mobile workforce of today by bringing collaboration to a whole new dimension (Brender & Markov, 2013). CC refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centres that provide those services (Armbrust et al., 2010). Another good definition on the term is the one provided by Gartner, defining cloud computing as "a style of computing where massively scalable IT-enabled capabilities are delivered 'as a service' to external customers using Internet technologies" (Heiser, 2009). The word "cloud", a metaphor for the Internet, was likely to have been inspired by internet illustrations which often depicted it as cloud images (Sultan, 2011)

Virtually all sets of actors in the IT sector including providers of access devices, providers of infrastructure, application and content services and providers of network connectivity are affected by the unfolding CC paradigm (Khanagha, Volberda, Sidhu, & Oshri, 2013). The network-centric model of computing, where all data, applications, and services are hosted on the network is a significant departure from the traditional client-centric model of personal computing, where data and software resources are hosted on a local computer, or the client-server model of organizational computing, where resources are hosted on organizational servers (Bhattacherjee & Park, 2014). Thus, CC is attractive to business owners as it eliminates the requirement for users to plan ahead for provisioning, and allows enterprises to start from the small and increase resources only when there is a rise in service demand (Zhang, Cheng, & Boutaba, 2010). In any case, and in spite of its challenges (Subashini & Kavitha, 2011; Wei & Blake, 2010), CC technologies have gained momentum and moved from a hyped trend to a mature set of technological innovations providing infrastructures for business (Jiménez-Domingo, Gómez-Berbís, Colomo-Palacios, & García-Crespo, 2011). However, CC, research is still in its early days (Bhattacherjee & Park, 2014) and more studies on its adoption, government, and evolution are needed (Prieto-González, Tamm, & Stantchev, 2015; Rebollo, Mellado, Fernández-Medina, & Mouratidis, 2015).

Cloud computing can be categorized as public cloud, private cloud and hybrid cloud in terms of deployment (Wang, Zheng, Lou, & Hou, 2015). A public cloud is available to the general public in a pay-as-you-go manner (Armbrust et al., 2010). Normally, many customers share an infrastructure. The customer has no influence on compliance or security aspects. The services are accessed via internet, the applications are, in the most cases, very standardised products (Petruch et al., 2011). A public cloud has the advantage that the available space and computing power is almost unlimited and quickly available (McCafferty, 2010). Public clouds can make it very easy to respond fast to customer demand in different geographies and markets. Using the public cloud can decrease further IT investments dramatically (Petruch et al., 2011). But public clouds are under suspicion to be unsecure. The risks for a company in the context of CC can be observed in three areas: confidentiality, integrity and availability (Jaster, Mendonca, Slamka, & Radmacher, 2010). Finally, hybrid cloud allows companies keeping their critical applications and data in private while outsourcing others to public. The benefits and drawbacks of such approach have been discussed in deep in the literature e.g. (Chou, 2015; Garrison, Wakefield, & Kim, 2015; Laatikainen, Mazhelis, & Tyrvainen, 2016).

Focusing on private clouds, these are self-owned (or, more precisely, exclusively used) IT infrastructure, including computers, storage and software, of the enterprises (Petruch et al., 2011).

This infrastructure is provided as a virtualised service to end users in the company and runs behind a corporate firewall (Hall, 2009). This reduces some concerns about data privacy but on the other side also diminishes some of the important advantages of CC: the company still has to manage the whole infrastructure itself resulting in higher operational costs (Armbrust et al., 2010). Furthermore, the company cannot benefit from extensive statistical multiplexing in order to ensure very high utilisation (Petruch et al., 2011). The organization may or may not own the physical infrastructure and can be managed by the organization itself or by a third party moreover, private cloud may or may not be located at organization's site. However, private cloud is for the use of only single organization and the resources are not utilized by any other customer (Ali, Khan, & Vasilakos, 2015).

The typical provision models of CC differ depending on the architectural level of the provided services. There are three general types:

- Software as a Service (SaaS). SaaS is a multi-tenant platform that uses common resources and a single instance of both the object code of an application as well as the underlying database to support multiple customers simultaneously (Rimal, Jukan, Katsaros, & Goeleven, 2011).
- Platform as a Service (PaaS). Provides the facilities required to support the complete lifecycle of building and delivering web applications and services (Subashini & Kavitha, 2011). Compared with conventional application development, PaaS can significantly reduce the development time, and also offers hundreds of readily available services (Rimal et al., 2011).
- Infrastructure as a Service (IaaS). It is the delivery of computer infrastructure as a service (Subashini & Kavitha, 2011). This model is advantageous to business users, since they do not need to invest in building and managing the IT systems hardware to take advantage of the latest technology; apart from

greater flexibility, a key benefit of IaaS is the usage-based payment scheme (pay as they grow) (Rimal et al., 2011).

An organization has to manage (govern and control) the cloud services it uses – both the ones that are used internally (e.g., invoice processing, office automation) and externally for the interaction with customers (e.g., Customer Relationship Management or e-commerce platforms). This governance responsibility is typically expected to be provided by the CIO or the head of IT and is often considered the main added value of an IT department in a cloud-oriented scenario (Petruch et al., 2011). A meaningful approach for the IT department to provide cloud governance can be the extension of traditional governance frameworks to CC as proposed in (Stantchev & Stantcheva, 2012, 2013). Due to the fact that the data ownership lies within the operating department, the responsibility for the fulfilment of the compliance requirements lies there as well.

To sum up, CC is a key topic in IT research today, both in the technical and in the managerial side. However, governance and compliance as well as privacy issues are still a challenge for researchers and practitioners alike.

2.3 Compliance requirements

The term *compliance* presents several meanings. Focusing on the topic of this doctoral thesis, according to the MacMillan dictionary, compliance is the practice of obeying a law, rule, or request. This definition is close to the one provided in the Cambridge Dictionary, in which the term is defined as the act of obeying an order, rule, or request. In the Oxford dictionary it is defined as the action or fact of complying with a wish or command. Finally, in the Merriam-Webster dictionary, compliance is defined 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.

According to Kim (2007), IT compliance means an accordance of corporate IT systems with predefined policies, procedures, standards, guidelines, specifications, or legislation. Another good definition of the term, this time focussed in the human factor, is as follows: the extent to which employees follow organizational IT policies to appropriately use the target IT in their job (Liang, Xue, & Wu, 2013).

IT compliance is a higher level concept encompassing both IT use and mandatory elements specifying how IT should be used (Xue, Liang, & Wu, 2010). IT is becoming compliance-driven and the days of freelance activities are gone – replaced by internal controls, documentation, audits and oversight that are leading to “compliance paranoia.” (Lawton, 2007). However, these changes are not superficial. These regulations on IT direction and management have the ability to disrupt business; no matter the source of the demands (government, courts or industry trade groups), organizations are being encouraged (and often required) to have IT internal controls and to disclose these to the requesting parties (DeLuccia IV, 2008).

The consequences of not complying with these laws can be devastating and may include substantial fines, financial losses, lawsuits, customer dissatisfaction, and loss of reputation and market confidence (Hamdaqa & Hamou-Lhadj, 2011).

From government mandates such as the Sarbanes-Oxley Act of 2002 to meeting quality guidelines such as COBIT (control objectives for information and related technology) and ITIL, organizations are learning to adapt their IT development and delivery process so that it becomes a true business process that can be tracked, measured, repeated, and cost controlled (Ragan, 2006). Thus, the inevitability of coping with compliance pressures identifies a need for new IT and IS solutions to compliance management and denotes a need for evolution of current IT and IS approaches such that they are better able to support the fast-changing regulatory compliance management field (Abdullah, Sadiq, & Indulska, 2010). However, and given the different regulations and frameworks, meeting multiple control framework requirements can be costly and inefficient due to similarities between various frameworks that produce redundancy and duplication of effort in the organization's compliance initiatives (Hayden, 2009). In other words, there is a need to investigate ways to help IT companies manage a large number of possibly overlapping or conflicting regulatory compliance requirements (Hamdaqa & Hamou-Lhadj, 2011). There are several efforts in the literature studying the phenomenon from diverse perspectives including, among others, education (Harris & Cummings, 2007), norm activation (Yazdanmehr & Wang, n.d.), gamification (Baxter, Holderness, & Wood, 2016) or employee performance (Liang et al., 2013). There are also some works devoted to the analysis of IT compliance from a framework perspective (Kim, 2007; Schlarman, 2007). Last, communities of practice have been pointed out as one of the solutions to negotiate and refine explicit meaning from diverse opinion and formal knowledge on regulations (Breaux, Antón, Boucher, & Dorfman, 2009). The importance of the topic has been recognized in the formulation of a new role inside organizations: IT compliance manager (Ang, Joseph, & Slaughter, 2015).

Compliance requirements can result from both internal and external regulations. Internal regulations include guidelines or operating procedures. External regulations are usually in form of laws, regulations or civil contracts (Kim, 2007). Additional considerations arise from industry-specific requirements, i.e. for banks, insurance companies and the public and healthcare sector. A timely identification of all compliance requirements is often one of the first steps of an outsourcing project and an important milestone for the project's success. For the usage of cloud services these requirements come with a higher level of complexity. This complexity depends on the data type and the cloud service structure and service. In CC, there is a need of an in deep analysis concerning IT compliance to support its adoption (Brehmer & Seitz, 2015)

2.4 Frameworks in IT management and governance

When assessing research on frameworks for IT governance there is a pattern of approaches that propose the extension of already existing frameworks to address cloud-specific aspects (Lawler, Joseph, & Howell-Barber, 2012; Stantchev & Stantcheva, 2012, 2013), typically by using approaches aimed towards service-oriented computing (Wei & Blake, 2010) or web services (Ferris & Farrell, 2003) as an intermediary. Sometimes these frameworks were created originally for service-oriented computing or web services (Lawler et al., 2012; Stantchev & Malek, 2011) and sometimes the usage of more general frameworks such as ITIL and COBIT is proposed (Stantchev & Stantcheva, 2012, 2013). Other initiatives include ISO/IEC 38500 and Capability Maturity Model Integration for Services (CMMi-SVC) (CMMI Product Team, 2010).

Results of the usage of these approaches in CC environments are often inconclusive. For instance, in (Lawler et al., 2012) authors state that "Even though the cloud computing projects and systems in the analysis clearly contributed benefits of convenience and efficiency to the business firms and organizations, the development was not largely enabled by a disciplined method." One of the most ambitious studies of governance aspects for CC asked explicitly about the role of reference frameworks such as ITIL and COBIT with approx. 21% of organizations answering that they consider such frameworks relevant for the governance of cloud services (Petruch et al., 2011).

A more detailed analysis of the usage of information security frameworks (being a more specialized type of IT governance frameworks) in the context of CC is presented in (Rebollo, Mellado, & Fernández-Medina, 2012). There authors aimed to identify relevant frameworks by conducting a structured literature review in relevant online databases, including Science Direct, Elsevier, Google Scholar, IEEE, and the ACM Digital Library. Keywords related to cloud were used with a specific subset of controls from the ISO 27000 family serving as an additional inclusion criterion. Only works published after 2006 were considered. The authors identified the following relevant frameworks:

- Cloud Computing: Benefits, risks and recommendations for information security – a guide from The European Network and Information Security Agency (ENISA) (Catteddu, 2010);
- The Cloud Cube Model – a model for selecting cloud formations based on security objectives that is presented scholarly in (Chang, Bacigalupo, Wills, & De Roure, 2010);
- Cloud Security and Privacy – a rather general introduction to a range of security-related aspects of CC published in (Mather, Kumaraswamy, & Latif, 2009);
- IT Control Objectives for Cloud Computing – the specific view from ISACA – the organization responsible for COBIT – on the subject (Lageschulte et. al., 2011);

- Security Guidance for Critical Areas of Focus in Cloud Computing – a guide provided by the Cloud Security Alliance (Reed, Rezek, & Simmonds, 2011);
- Security and Control in the Cloud – a proposal to actually adapt the information security management system (ISMS) concept from ISO 27001 to a "virtual" ISMS that includes services that are outsourced to cloud providers (Julisch & Hall, 2010).

Results of the assessment of these frameworks confirm that "… current information security governance (ISG) frameworks deal with most of the proposed criteria to some extent, gaps have been detected that must be filled" with "deficiencies found in the process adaptation, audit and SLAs criteria." (Rebollo et al., 2012).

A more recent study on the topic is devoted to compare and integrate related models like COSO, ITL, ISO 27000/9000, ENISA and COSO (Becker & Bailey, 2014) to draw the initial steps of a framework named IT Cloud Governance Dial. More recent developments include non-specific frameworks for governance and risk management and Cloud Controls Matrix V3 Framework from Cloud Security Alliance and the ISO/IEC 38500:2008 (Chaudhuri, 2015, p. 2008), an initiative that is not presenting conclusive results yet.

2.5 Legal Environment for Compliance

This consideration looks at the intricate legal requirements associated with compliance using the particular example of health-related data in German jurisdiction. Health-related data is particularly well fitted to show the complexity of regulations as it is considered a particularly critical data asset.

Whether in the public administration, in a company, at the general practitioner's (GP) office or in the medical insurance – almost every institution needs to process personal data. There is a wide range of applicable regulations that govern the protection of individual rights and the right to informational self-determination of humans.

Of special relevance at the European level is the EU General Data Protection Regulation (Regulation of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data). This regulation defines in § 4 EUDSV the term of personal data. In addition, other elements – for example, the data subject's rights, rules for data controllers and their duties, order processing, cooperation with regulators and data security, reporting and notification obligations, the privacy risk management and international data transmission are regulated by the document. The regulation was approved on April 27-th 2016[1]. Data protection and information

[1] http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.DEU&toc=OJ%3AL%3A2016%3A119%3ATOC

security aspects of transatlantic (Europe-USA) data handling were regulated until October 6-th 2015 by the "EU – U.S. Safe Harbor" framework, adopted in 2000 by the European Commission. Then the European Court ruled this framework inapplicable. Currently, there is a follow-up framework called the EU – U.S. Privacy Shield which was adopted by the European Commission on July 12-th 2016[2].

At national level, there is currently a large number of laws on data protection. In Germany, for example, the applicable Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) defines personal data in § 3, Section 1 but it goes further to define also health data in § 3, Section 9 as a special type of personal data with legally mandated increased protection requirements. The collection, processing and use of health data is in general allowed only for the purposes of preventive medicine, medical diagnosis, care or treatment, or for the purpose of managing and administering health services. Such data can be processed only by medical personnel or by other persons that possess the same appropriate confidentiality obligations (§ 28 BDSG, Section 7). A pre-assessment of the legality of this data processing should be conducted by the company data protection officer (§ 4e BDSG No. 1, Section 5).

During operation of IT systems which process health data, both the original organization (e.g. hospital, practitioner, insurer) and the outsourcing company should implement a number of appropriate technical and organizational measures of precaution stemming from a catalog of eight control requirements (§ 9 in conjunction with the annex to § 9 BDSG). There is a similar requirement for socially-related data in §78a of the Social Codex (Sozialgesetzbuch, SGB), in conjunction with the annex to §78a SGB.

The law stipulates only general requirements, the definition and implementation of specific measures is the obligation of the specific organization. For example, it should apply general measures for protecting personal data (e.g. limited access) also with respect to health-related data and it can further extend them with measures to protect data transmission (e.g. encryption). Furthermore, systems that are operated for more than one client (e.g., processing appointment data or analysis data for multiple GPs) should ensure strict separation between data of each client organization. There exist specific recommendations about the compliant operation of a hospital management system (HIS) (Hasse, 2012). Similar requirements apply for CC and outsourcing scenarios, as providers are expected to implement and assure security requirements of the client organization.

Specific requirements are derived from regulations in the area of medical confidentiality, social data, and state-specific rules (rules that are different in every specific German federal state, e.g. Bavaria or Hamburg).

Medical confidentiality ensures the trusted relation between a doctor and a patient. In Germany this relation is regulated in the professional code of conduct for doctors

[2] http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm

(*Muster-Berufsordnung für die deutschen Ärzte und Ärztinnen* - MBO-Ä) with medical confidentiality specified in § 9 Section. 1 MBO-Ä. A breach of confidentiality is considered a criminal offense and a reveal of patient data can result already from archiving patient data with a service provider without the prior written consent of the patient. This prior written consent should include the specific data and the legal information about the service provider and is therefore often unfeasible.

Social data denotes all personally-related data that concerns social aspect of a person. The increased confidentiality requirements with respect to it are defined in § 35 Sect. 1 SGB I. A specific example of regulations in this area is the recently introduced "electronic health card" (*elektronische Gesundheitskarte*, eGK). Requirements concerning data protection in the context of the eGK are specified in Volume V of SGB, with particular regulations concerning encryption and access control lists (ACLs) in § 291a SGB V. In order to assure compliance, the newly founded joint venture of German health insurers – gematik – has specified an extensive security concept that will also be applicable to CC providers and other outsourcing providers that will work with the eGK [3].

Hospitals in Germany are particularly affected by state-specific rules with respect to data protection and information processing. A variety of state-specific hospital laws exist that often stipulate different requirements with respect to patient data processing. Let us consider the state hospital law (Landeskrankenhausgesetz, LKG) of Berlin and the state health data protection law of North Rhine-Westphalia (*Gesundheitsdatenschutzgesetz*) as examples. They both include regulations regarding data transmission and reveal of data. For example, hospitals in Berlin are only allowed to process patient data in-house or to outsource this processing to another hospital. Other providers can process patient data under the mandate of the hospital only if they prevented to map the data to a certain person or to derive person-related aspects from it (§ 24 Sect. 7 (2) LKG Berlin).

In summary, the assessment of legal regulations shows, that all person-related data (and particularly medical data) in CC and other outsourcing scenarios should be protected from access by the service provider or other unauthorized third parties. In practice, this requires the encryption of the data, so that it cannot be encrypted by the service provider, or, alternatively, the anonymization or pseudonymization of the data.

Furthermore, tax regulations often include specific regulations regarding invoices, balance sheet data and other related data assets.

Outsourcing in the context of CC typically constitutes the soc. data processing under mandate (german: *Datenverarbeitung im Auftrag*) as stipulated by § 11 BDSG. This results in specific requirements regarding the contractual relationship between client and service provider. It should specify the type and scope of the intended use

[3] http://www.gematik.de/cms/de/spezifikation/abgekuendigte_ releases/release_2_3_4/release_2_3_4_datenschutz/datenschutz/release_2_3_4_sicherheitskonzept.jsp

of data, the control rights of the client, as well as the specific technological and organizational measures that the provider will be implementing in accordance with § 9 BDSG. Furthermore, prior to the start of the actual data processing under mandate, the client has to carefully select the service provider and to convince himself that the technological and organizational measures are appropriate (§ 11 Section 2 (4) BDSG). This control obligation can be fulfilled not only in person but also through the use of experts, ISMS auditors, requirement of self-disclosure forms from the provider, as well as requiring certificates or proofs of established data protection concepts from the provider. Non-compliance with this control obligation can result in regulatory fines. This control obligation continues during the actual data processing with a requirement of regularly controls. The frequency of such follow-up controls differs in accordance with the scope of data processing, the associated risks, the innovation cycle of related technologies, as well as the sensibility of the processed data. Relevant CC providers in Germany conduct yearly audits by independent audit organizations and make the audit reports available to their clients.

2.6 Chapter Summary

This chapter presented the state of the art research in the areas of change management in IT, outsourcing and cloud services, compliance requirements, frameworks in IT management, and also discussed the legal environment for compliance.

In the area of change management, it was shown that various initiatives consider change management to be a key issue for IT Service Management and this process is, based on the results from the literature review, part of the most important initiatives in the field. However, currently there are no substantial research activities reported that analyze in deep the connection of change management with compliance management.

In the area of outsourcing and cloud services, it was shown that CC is one of the most important topics in IT and IS research today, both in the technical and in the managerial side. However, governance and compliance as well as privacy issues are still a challenge for researchers and practitioners alike and there is a specific gap between research approaches proposed and their application in industry.

In the area of compliance requirements, it was shown that compliance requirements can come from very diverse sources and there are approaches that focus on soliciting them from specific areas. Furthermore, it was shown that compliance of CC adds additional complexity as compared to traditional IT provisioning scenarios and that CC adoption depends heavily on solid compliance assessments. What is missing, is an approach that targets CC compliance specifically and also accounts for the fast changing technologies in this field.

In the area of frameworks in IT management, the literature assessment showed that there is a pattern of approaches that propose the extension of already existing IT management or governance frameworks to address cloud-specific aspects. Some of them are focused more on technical and architectural aspects such as web services, while others consider organizational and processual aspects as predominant (e.g., ITIL). Specific frameworks were identified that can provide relevant contributions to the envisioned framework, while it was confirmed that there are gaps and deficiencies regarding process adaptation, audit and SLAs, which all are directly intertwined with change management.

Concerning the legal environment for compliance, it was shown that – somewhat counterintuitively – the legal environment is not clearly delineated so that it is clear what rules apply. On the contrary, various legal requirements exist at the regional, national, and international levels and also depend on sector, organizational type and purpose, and on many other specific aspects. There are particularly stringent regulations regarding processing of highly sensitive data in specific sectors such as healthcare. Thus, there is a need for an approach that accounts for the broadness and diversity of applicable legal requirements that is also capable to solicit, examine and compile them as a coherent set of rules that need to be obeyed in order to ensure compliance.

The framework that will be developed, validated, evaluated, and assessed in the next chapters aims to fill the gaps that have been identified in all these areas by proposing a holistic approach. It will extend the research body of knowledge by providing an artefact that can be examined, assessed and developed further by other researchers in the field. This artefact – the envisioned Compliance Framework for Change Management in Cloud Environments – is the objective of this work.

The Governance, Risk and Compliance (GRC) area is one of the critical management areas for every organization. This is particularly the case for information technology (IT) departments where both human resources and technical infrastructures (software and hardware) need to work seamlessly in order to provide the expected benefits. The study of the literature shows that sound GRC methods are key to running and maintaining secure and compliant computing infrastructures.

An important and particularly challenging aspect of the IT landscape is its constant and perpetual evolution in order to keep pace with new and emerging technologies that find their way faster and faster into the organizational infrastructure. Since assessments of risks and compliance aspects always refer to a certain (more or less static) situation, such frequent changes pose a real danger to the overall relevance of these assessments in the mid and long-term perspective. So, a sound approach to ensuring compliance not only punctually (both in time and space) but holistically – considering the complete IT landscape in a continuous way – needs to integrate with the change management function of the organization.

Another important development in the last eight to ten years was the emergence of Cloud Computing (CC) as a straightforward and efficient way of providing IT functionality to organizations. While it poses many various challenges to IT management in general, CC is particularly relevant for GRC as it makes an IT provision approach that was previously sometimes applied – outsourcing – to a predominant approach to provide infrastructure (called Infrastructure-as-a-Service or IaaS), platforms (called Platform-as-a-Service or PaaS), and software (called Software-as-a-Service or SaaS) within an organization.

CC and outsourcing entail wider challenges for GRC as it involves the inclusion of an external party as a service provider within an organization reflecting specific aspects of provider selection, contract management, service level agreements (SLAs), and monitoring. They become even more challenging in the context of frequent and interdependent changes. Therefore, this thesis is aimed at the definition and validation of a Compliance Framework for Change Management in Cloud Environments (short: CFC MCC). The proposed solution of the problem has been approached from a multidisciplinary point of view taking in consideration aspects from computer science, IT management and IT governance, but also such aspects as legal and cultural dimensions. The proposed solution provides a framework to support the solicitation of requirements from different subject areas (e.g., organizational, technological, cultural) and their subsequent consideration within the change management process of established IT management frameworks such as ITIL. It can be tailored to the specific situation of most organizations and provides a consistent approach to address GRC aspects in rapidly evolving cloud-based organizational IT landscapes.

The development of this thesis has followed a sound, consistent and rigorous research methodology that has included a systematic literature review and qualitative methods and quantitative methods. The scientific discourse within the thesis has been structured following best academic practices and recommendations. In the last phase of the research methodology an empirical validation has been performed to verify the applicability of the framework. The data obtained from the validation indicate that the application of the framework for ensuring compliance in CC environments constitutes a relevant improvement of the change management process.

3 Problem formulation and research approach

In this chapter, the problem to be solved is identified and explained. Secondly, the approach to solve the problem is presented. This second section presents the research approach, design, and methodologies to address the research problem behind them, followed by a justification of the research methodology and the adopted research method are presented. Finally, a set of limitations on validity are presented and justified.

3.1 Research Problem

The importance of CC for organizations is unquestionable and will become even more important in the coming years as both academics and IT consultants have underlined. Successful deployment in CC denotes the realization of unique or valuable organizational benefits that are a source of differentiation and competitive advantage (Garrison, Kim, & Wakefield, 2012). However, given the inherent change in IT panorama, compliance, one of the most important aspects in IT, is not an easy task that is even more complicated in outsourced environments like CC. According to Subashini and Kavitha (2011), CC is shaping the future of IT but the absence of a compliance environment is having dramatic impact on cloud computing's growth. Within compliance aspects like cloud data provenance, metadata management and jurisdiction are still an open issue (Pitropakis, Darra, Vrakas, & Lambrinoudakis, 2013). The nature of CC raises all kinds of compliance problems (van de Weerd, Mangula, & Brinkkemper, 2016). What makes compliance difficult for CC providers is the sheer number and complexity of laws and regulations that need to be understood and enforced in their systems (Papanikolaou, Pearson, Mont, & Ko, 2014). In a recent study, several compliance issues in CC environments have been analyzed (Yimam & Fernandez, 2016). This study reveals that more research is needed to overcome compliance challenges and their solution.

Change management is seen as a way to approach the problem combining business perspectives and impact assessment. In CC settings, change management has been pointed out as an approach to solve some of the issues on its adoption and further development in several aspects (Martens & Teuteberg, 2012; Owens, 2010; N. Sultan, 2013). Although there are some approaches to solve compliance in CC in a partial way (Papanikolaou et al., 2014), to the best of author´s knowledge, there is not a holistic and integrated way to manage the adoption of such approach. Thus, it is perfectly defined the problem object of study of this thesis: the application of change management defined under governance principles to conformance problems in CC.

3.2 Research Approach

The objective of this thesis is the definition of a compliance framework suited to outsourcing projects and the operating phase in a cloud service environment. This framework will include a method for developing, evaluating and analyzing requirements and defining required measures and controlled procedures. The main focus will be on the change management process during the project and operation phase. The compliance framework will help to improve changes, to reduce the risks and to fulfill almost all legal requirements. The results of the function of the framework will be statistically analyzed to test its applicability and overall success.

The resolution of the problem that this doctoral thesis is facing requires a set of steps and elements that must be followed in order to build a solution to the problem useful and generalizable. It is also needed to adopt a sound scientific approach to achieve this solution. This leads us to the need of a research methodology. A research methodology can be defined as the aggregation of several methods, assumptions, models, techniques that constitutes the procedures for collecting and analyzing the data, measuring progress and research success in order to solve a research problem (Panneerselvam, 2014). The selection of a research methodology is resultant from different factors including, time, resources, industrial accessibility, the known and unknown variables, previously conducted research and known theories from the field and lastly research goals and questions (Creswell, 2013). As a consequence of the objectives of the doctoral work and the research questions formulated, the adoption of a blended qualitative and quantitative method approach is indicated.

Since the purpose of this thesis is the definition of a framework applicable to almost all kind of organization and to give answer to the research questions, different phases must be articulated to reach the final goals. This requires a set of steps and elements that must be observed in order to build a solution to the problem useful and generalizable, built upon a sound research approach. Thus, the approach to the problem must include two distinct phases, as shown in the next figure.

The first of these phases, Definition, and whose development is included in in Chapter 4 of this thesis, is aimed to define the factors that must be included in the framework including de different change categories that can affect CC in terms of compliance. Moreover, it is needed to develop an assessment tool and process for these categories and aspects. This first attempt is performed by means of an extensive literature review but it is also based in decades of professional practice in the topic from the Ph.D. candidate. Once defined, for every of the aspects demarcated, a set of qualitative studies will be devoted to support the first version of the framework with regards to the different categories, aspects and assessment method.

Once the first version is defined, the second phase is the validation of the framework in a Phase 0 study by a set of experts. The aim is to evaluate the overall validity of the instrument designed as part of the thesis along with obtaining previous feedback from experts on the framework towards an eventual improvement. This is included in the Chapter 5 of this document.

The third phase is the improvement of the framework taking into account the improvements suggested by experts in phase 2.

The last phase is the deployment of the framework in a set of cases studies. For evaluating the contribution of this work, two different case studies were conducted. The framework is intended to come into practice by applying its principles to different business domains. These case studies are aimed to demonstrate the ability of the framework to be agnostic to any business domain regardless of the CC setup and functional scenario. Both quantitative information taken from selected KPI and qualitative information will be analyzed to provide insights to the deployment of the framework.

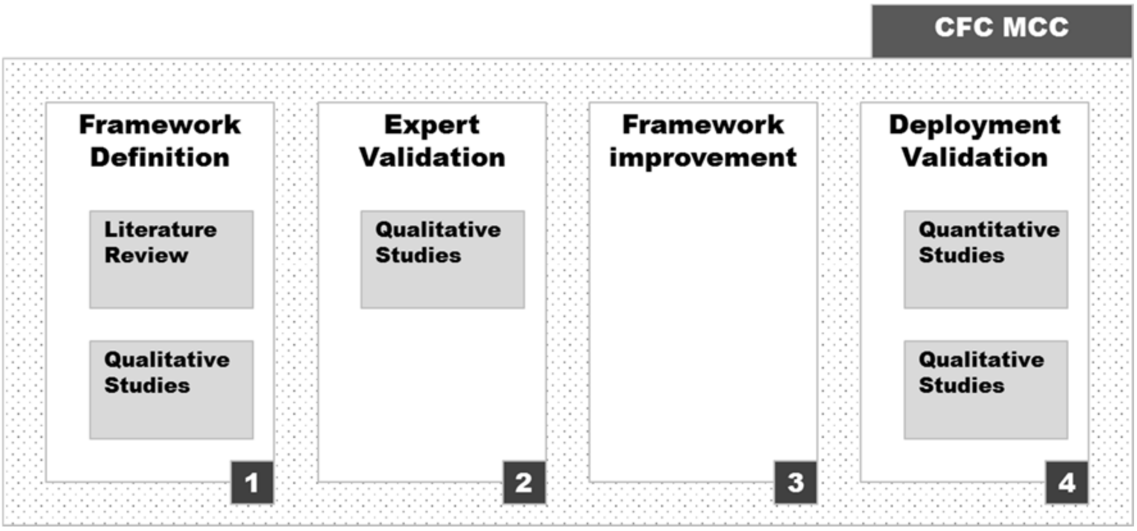


Figure 1. An overview of the proposed research approach

To the aims described in this chapter, we use a set of qualitative and quantitative methods. These methods include case studies, semi-structured interviews, focus groups, statistical techniques and quantitative analysis.

Regarding case studies, they are characterized by their flexible nature, evolving over the course of the study, focusing on a phenomenon in context, using multiple methods of evidence or data collection (Cruzes, Dybå, Runeson, & Höst, 2014). Case studies are in Information Systems discipline more mature than in Software engineering (Runeson & Höst, 2008) and are pervasive in the literature. Not in vain, case study research is the most common qualitative method used in information systems (Dubé & Paré, 2003; Myers, 1997). In a nutshell, a case study is a multi-dimensional tool that is frequently used for seeking answers to specific research inquiries. A case study does not require a researcher to have ability to control over the events and situation like action research does (Oates, 2005). This set of reasons lead us to the adoption of case study as the main vehicle for the assessment of the framework.

3.3 Limitations on validity

Until now the problem has been enunciated in a generic way. The solution proposed in this thesis is designed assuming a set of limitations related to the conditions the environment. The purpose of this section is to analyse the different threats of validity regarding Design Validity, Analytical Validity and Inferential Validity. Taking into account that the construction of the framework is performed using qualitative methods, these are the measures to take into account for this work. However, and confronting with quantitative approaches, the issue of validation in qualitative research is rather ambiguous and contentious (Ridenour & Newman, 2008). Validity, in the context of a qualitative study, is defined as the extent to which data are plausible, credible, and trustworthy, and thus can be defended when challenged (Venkatesh, Brown, & Bala, 2013). Agreeing with (Lincoln, Lynham, & Guba, 2011), we organized different types of validity for this work: credibility (as opposed to internal validity of quantitative research); transferability (as opposed to external validity of quantitative research); and confirmability (as opposed to statistical conclusion validity in quantitative research).

With regards to credibility, this involves establishing that the results are believable from the perspective of the participants in the research to convincingly rule out alternative explanations. Researchers consider that the variety of organizations involved in the case study were enough to reduce their influence in results. Additionally, it is possible to asseverate that all experts had comparable levels of knowledge and experience. Given that respondents were in all cases chosen because of their expertise and experience, authors made sure that experts possessed a comparable level of knowledge and expertise.

Concerning transferability, which is related to the generalisability of research findings, two possible threats are assumed. The first is the limited number of participants in the case study. Although this threat exists, making difficult the generalization of results, it is also true that the two case studies are representative enough to describe the applicability of the framework. The second threat is rooted in the fact that the sample was not taken randomly. It is assumed that generalisation of results is not guaranteed, however the framework and the context and working conditions are not uncommon, so similar implementations are possible for replication.

Finally, confirmability is the degree to which the results could be confirmed or corroborated by others. According to (Wester, 2011), there are several factors that can influence confirmability results including the thoroughness of one's field notes, summaries, and theoretical notes, which provide an "audit trail" and the transparent nature of the biases of the researchers. To avoid this bias, an auditor was assigned to the process to assure the quality of the study.

With regards to the validation of the framework, this is performed using a quantitative approach. The purpose here is to analyse the different threats to the study conducted regarding conclusion validity, construct validity, internal validity and external validity.

Content validity is the degree to which items in an instrument reflect the content universe to which the instrument will be generalized (Boudreau, Gefen, & Straub, 2001). This aspect was verified by checking the meanings of variables and by a careful literature review. To ensure content validity, the first version of the questionnaire was sent to experts to assess it. This resulted in several changes regarding the wording of questions.

Conclusion validity is concerned with the relationships between dependent and independent variables, that is, the provision of statistically-correct conclusions based on correct measures and appropriate statistical analyses. In the case of this study, authors considered that the sample and its size were convenient and significant enough to test the proposed research questions. However, authors also assume that sample is limited.

The internal validity is concerned with factors that may affect dependent and which are out of researchers' control. In this case, authors believe that this threat should come from the fact that subjects may not have comparable levels of knowledge or expertise. Given that respondents were in all cases chosen because of their expertise and experience, the authors tested whether both group of students possessed a comparable level of knowledge and expertise. One-way ANOVA was used to compare the means of factor scores between the two groups. No significant differences were found, suggesting that the type of respondent and organization did not cause any survey biases.

Construct validity is the extent to which a construct measures the concepts that it purports to measure (Straub, 1989). It presents two different components: convergent and discriminant validity. Convergent validity assesses consistency across multiple constructs, while discriminant validity examines whether different constructs diverge from one another. Furthermore, construct reliability measures the degree to which measures are free from random error, and therefore yield consistent results. As reported earlier, multiple tests to ensure construct validity and reliability were performed.

External validity refers to the extent to which research findings can be generalized, and to what extent the findings are of interest to other purposes. Regarding external validity, two different threats are assumed. The first is the size of the sample, which can complicate the generalization of the results. The second is the fact that the sample was not taken randomly.

4 Compliance Framework for Change Management in Cloud Environments

The previous chapters have established the need for a framework that combines aspects coming from the specifics of change management in the field of IT, the peculiarities and challenges of outsourcing and CC when compared to traditional ways of providing IT services within an organization. Furthermore, the framework should account for compliance - both IT compliance and compliance of the overall organization with applicable regulations, while – in the same time – provide a special focus on legal aspects of this compliance.

Moreover, this framework should be established following a sound scientific approach and best academic practices. It should also be validated and evaluated with scientific rigor in order to establish its merits for accomplishing the challenges it claims to solve.

When considering the different aspects that should provide input to the envisioned framework and their specifics, it is reasonable to define different subject areas that serve as sources to emerging reasons of change. First, these reasons need to be gathered, solicited and structured for each subject area. Following that, the reasons coming from all subject areas should be merged, cleaned, decomposed and consolidated into a coherent set of requirements.

This chapter will first present a top-level overview of the proposed framework in order to accommodate the reader with the general paradigms that characterise it. Then the chapter will look into the motivation for the framework by presenting reasons stemming from state-of-the-art schools of thought in the relevant areas of computer science, information systems, management systems and standards, as well as mapping approaches. Following this, the approach for conducting the qualitative studies within the chapter will be presented.

Then the chapter will build up every one of the subject domains of the framework following the approach already specified in Chapter 3. Specifically, for every subject domain the assessment of its relevance from the point of view of current research, its elaboration in accordance with this state-of-the-art, the specific artefact that is developed, as well as a qualitative study to decide on the robustness of the artefact will be presented.

The final part of the chapter will describe the process of integrating the results from the different subject domains into a coherent set of requirements.

4.1 Overview of the Framework

The purpose of this section is to introduce a framework aimed to integrate change management with compliance management in a CC environment in order to provide organizations with a solution to address the topic in a sound way.

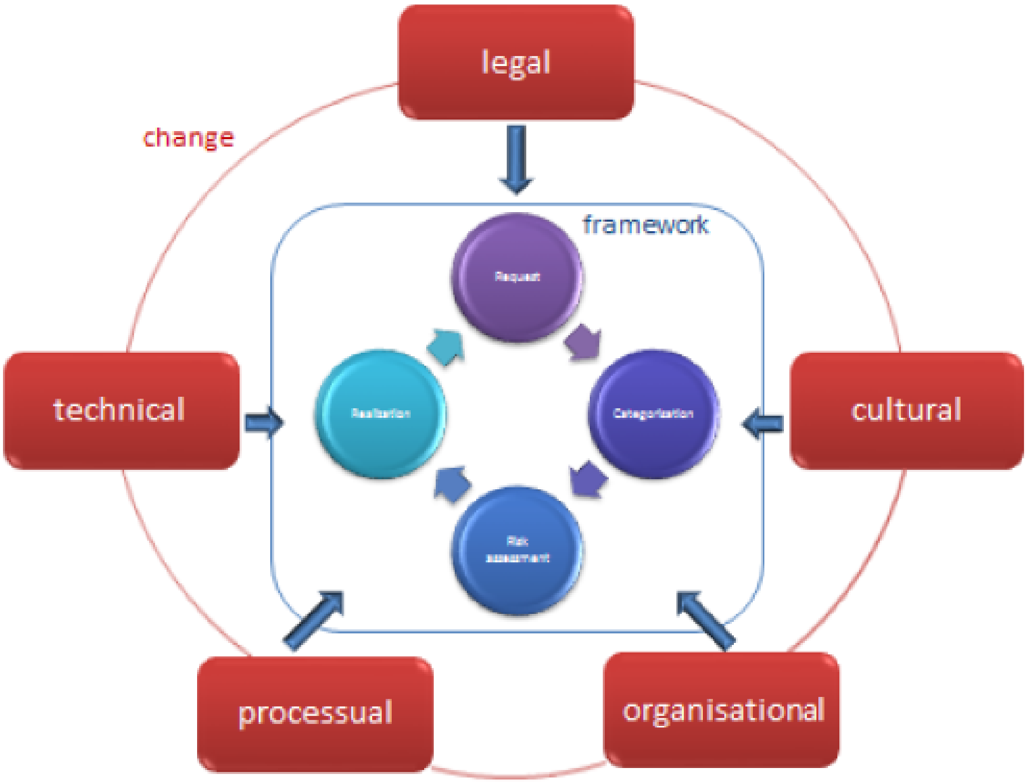


Figure 2. A schematic overview of the proposed framework

Figure 2 shows an overview of the proposed Compliance Framework for Change Management in Cloud Environments (short: CFC MCC) for cloud services. It builds on the lifecycle-oriented approach presented in (Stantchev & Malek, 2011) and extends them with a classification of emerging changes based on the PESTEL (Shilei & Yong, 2009) environmental analysis approach – the red areas on the outskirt. The management of the change requirements themselves is an adaptation of the general change management process already presented in Section 2.1. All these topics are assessed from CC perspective and compliance perspective – both embodied in the circle in the middle of the figure.

The overall framework structure depicted in Figure 2 aims to provide several important benefits. First, the consideration of change categories based on the origin of change necessity (e.g., legal, as already discussed in Section **Error! Reference ource not found.**, or organizational) will provide a necessary extension to the already accounted for categorization in accordance to how change comes about: planned, emergent, contingency, and choice (By, 2005). Furthermore, it will consider both external and internal triggers for change. The cloud-specific view will provide special consideration of CC-related aspects as already discussed in Section 2.2. The compliance-specific view will integrate the relevant areas that were presented in Section 2.3, while the detailed design of the individual process steps will incorporate select topics from the frameworks discussed in Section 2.4.

4.2 Motivation

The structure of the proposed five areas (legal, organizational, processual, technological, and cultural) from which the framework should derive requirements has been considered carefully. There are several groups of reasons that can be structured as follows:

- reasons stemming from the state-of-the-art research in computer science and information systems,
- reasons stemming from paradigms employed by management standards for information systems, and
- reasons derived from mapping approaches for management and process standards.

In the following subsections these groups of reasons will be elaborated.

4.2.1 Reasons stemming from the state-of-the-art research in computer science and information systems

In information systems research and relevant computer science fields the question of combining IT and real world objectives has been central from the onset. Shannon considered communication theory from the prism of the amount of information that can be transmitted through a given communication channel (Shannon, Weaver, & Wiener, 2009), while the abstract (but nevertheless definite) proofs of incompleteness of calculus by Kurt Gödel (Van Heijenoort, Frege, & Gödel, 1970) led to the consideration of computability by Alan Turing – first in the form of the Turing Machine (Turing, 2009) and later in the form of breaking the Enigma code (Mackintosh, 2008).

The idea to consider organizational aspects (e.g., processes and hierarchy/ structure) in the context of information technology is foundational for modern IT architecture concepts such as the concept of an Enterprise Architecture (Buckl, Ernst, Lankes, Matthes, & Schweda, 2008), and the concept of a service-oriented architecture (Stantchev & Malek, 2011). It is also central for the design of central organizational applications such as ERP systems (Law & Ngai, 2007).

The consideration of legal aspects is typical when an organization employs a compliance-oriented governance view (Dzombeta, Stantchev, Colomo-Palacios, Brandis, & Haufe, 2014). These legal aspects can serve as requirements for both organizational/processual aspects, as well as direct requirements of IT aspects. In the former case they define the legal context for IT indirect – via the detour through process and organization requirements, while in the latter they define the legal context for IT directly.

The consideration of cultural aspects has been put forward by the seminal works of Hofstede (Hofstede, 1983a, 1984) and is today considered as one of the most important areas of information systems research (Leidner & Kayworth, 2006).

4.2.2 Reasons stemming from paradigms employed by management standards for information systems

When assessing management standards for information systems, the consideration of processual aspects (processes or procedures) and organizational aspects (roles and responsibilities) is also very present. Furthermore, some of these standards also consider legal and cultural aspects specifically. In the context of the assessment of the research question relevant standards were examined about their specific coverage of the planned subject areas. The following table (Table 1) shows the results of this assessment for the most important related standards.

Table 1. Consideration of the Proposed Subject Areas (legal, organizational /processual, technological, cultural) in Relevant Standards

Standard	Relevant Sections	Subject Areas covered				Coverage	Relevance	Remarks
Name and Version		legal	organizational/	technical	cultural	in %	in %	
ISO 17021.2011	6 Structural requirements	X	X			100	80	Cultural is denoted as "social";

	9.1.2.2 Determining audit objectives, scope and criteria	X	X					applies to certification bodies
	9.2 Initial audit and certification	X	X	X	X			
ISO 20000.2011	4.4 Resource management		X	X	X	100	100	Cultural is denoted as “human”
	4.5.2 Plan the SMS (Plan)	X	X	X	X			
	4.5.3 Implement and operate the SMS (Do)		X	X	X			
ISO 27000.2016	2.16 control	X	X	X		100	100	Cultural is denoted as “social”
	3.5.2 Identifying information security requirements	X						
	3.5.3 Assessing information security risks	X			X			
COBIT 5 Ver2	Chapter 2. Principle 1: Meeting Stakeholder Needs	X	X	X		100	100	Cultural is denoted as “social”
	Chapter 3. Principle 2: Covering the	X	X	X	X			

	Enterprise End-to-end							
	Appendix E. Mapping of COBIT 5 With the Most Relevant Related Standards and Frameworks	X	X	X	X			

As exemplified in the table, all major relevant standards apply a similar view with respect to the structuring of subject areas. Furthermore, approaches that are following a lifecycle approach are also applying a similar view. One example is the software lifecycle approach tailored to small entities in the ISO 29110 standard (Larrucea, O'Connor, Colomo-Palacios, & Laporte, 2016; Larrucea, Santamaría & Colomo-Palacios, 2016; O'Connor & Laporte, 2014; Sanchez-Gordon, O'Connor, & Colomo-Palacios, 2015). Another example that follows a lifecycle approach for the management of a service-oriented architecture – the technological enabler of CC – also considers similar subject areas (Stantchev & Malek, 2011).

4.2.3 Reasons derived from mapping approaches for management and process standards

Of specific relevance for the verification of the proposed subject areas are approaches that aim to create mappings or identify process similarities between various management approaches and process standards. One very relevant work is the process similarity study presented in (Calvo-Manzano, Agustín, & Gilabert, 2008). There the authors propose a method for identifying the similarity among standards and models of best practices such as CMMI-DEV v1.2, PMBOK, PRINCE2, COBIT, and ISO 9001:2000. The method is called MSSS (Models and Standards Similarity Study method), and works at the process level. This already covers the proposed subject areas processual/organizational. Furthermore, at the detailed analysis level (when concerning more specifics) a correspondence template is suggested which includes the following elements for the specific mapping (to CMMI-DEV v1.2) presented in the paper: Inputs, Subpractices, Tools and techniques, Work products, and Informative Components, thus following a similar view of combining legal, processual/ organizational, technological and cultural aspects.

To summarize the argumentation for selecting the five subject areas (legal, processual/ organizational, technological and cultural) it can be stated that:

- This is a paradigm that is well established in current state-of-the-art research in computer science and information systems science,
- Most established management frameworks and practices (e.g., ISO standards, COBIT framework) follow a very similar approach with coverage being shown for several IT management related standards (see Table), and
- Mapping approaches in the areas of IT management and software process management also employ a paradigm that is matching the proposed subject areas.

4.3 Qualitative Studies using the Nominal Group Technique

For the purpose of the qualitative studies the methodology of the Nominal Group Technique (NGT) (Delbecq, Van de Ven, & Gustafson, 1975; Horton, 1980) will be applied.

The NGT essentially harnesses group facilitation processes in a manner that structures group interaction in specific tasks to achieve a specific goal. The NGT offers the possibility of obtaining a diversity of responses by minimizing group cohesion. Since responses are generated impartially from each participant and weighted equally, the data obtained with the NGT tend to provide a valid representation of the implicit views of the group (Elliott & Shewchuk, 2002). Factors that speak for NGT include its ability to allow balanced participation of all members of a group and the arrival at a final decision in a reasonable time. It has also been applied successfully in various domains including strategy planning and strategy development which makes it a good choice to address a problem domain with strategic ramifications for an organization. In the specific field of Information Systems research, NGT has been applied in the literature in a panoply of relevant and recent cases (Duggan & Thachenkary, 2004; Havelka & Merhout, 2013; Lederer & Mendelow, 1986; Parthasarathy & Sharma, 2014; Sutton & Arnold, 2013). Furthermore, its main purpose is decision making and – at that point of the thesis – a decision about the suitability of the proposed framework element is needed. Finally, this all will be done also for the overall framework.

The approach of NGT is typically conducted within a group of seven to ten individuals. For the qualitative studies within this chapter, the following general five step NGT process will be applied and possibly adapted where needed:

1. Silent generation – this is the step where every individual participant receives a written text with the stated task (the so called *Nominal Question*) and writes down his personal ideas about it in 10-15 minutes;

2. Individual round-robin feedback from group members on their ideas – here, every participant presents and explains his ideas to the others and ideas are recorded on a whiteboard or flipchart in 15-25 minutes;
3. Group clarification of each recorded idea – in this session, every single recorded idea is discussed and clarified within the group, typically within a structured group discussion in 20-30 minutes;
4. Individual voting and ranking on priority of ideas – in this session, every participant is provided with an *n* number of cards or stickers (with *n* being approx. 1/3 of the total number of ideas) where he needs to write down and rank the importance of the *n* most important ideas from the list; and
5. Discussion of group consensus results and focus on potential next steps – in this stage a consensus is being aimed with consensus types being total score of an idea (e.g., an idea gets a score of 8 from 3 experts and none from the remaining two experts for a total score of 24) or number of votes (e.g., only one idea is named by all five experts).

NGT, when applied stringently, can lead to consensus results in a limited period of time with sessions 4 and 5 being the ones where the moderator should try to avoid any unnecessary delays. The final discussion session is also important and it is often recommended that a clear vision of the next steps and the short- and long-term goals are crucial for a successful process. In the case of this thesis, the NGT will be applied in the qualitative studies related to the different parts of the framework. So, the short-term goals are to have robust artefacts, the long-term goals are to have a framework that really makes a difference, and the next steps will involve validating and evaluating the framework in the latter parts of this thesis.

4.4 Legal Environment

In the following, the relevance and the state-of-the-art approaches in the area of assessing legal environment will be discussed and subsequently elaborated. Then, the relevant framework element – *legal environment* – will be elaborated and the relevant artefact from the framework will be developed. At the end, NGT approach will be applied within a qualitative study to decide whether the artefact is robust enough.

4.4.1 Assessment of Relevance and Related Approaches

The legal environment is an important factor to have into consideration when defining a compliance framework. As it was presented in Section 2.5, just in the case of Germany and Healthcare, there exist a wide set of regulations defined to ensure data privacy and other issues such as assessment of policies. In general, protecting sensitive data from unauthorized users is an extremely important task that is regulated in a different way by means of legislation and enforcing laws in each country. The figure shows a brief summary on how different laws are applied to Cloud Data depending on the country where it is hosted (Leichter, 2014).

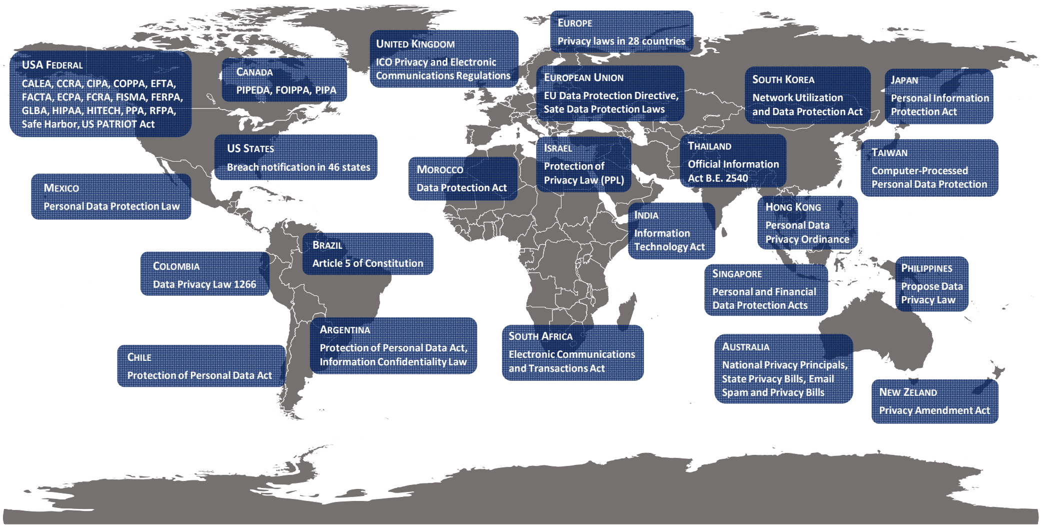

EUROPE
Privacy laws in 28 countries
UNITED KINGDOM
ICO Privacy and Electronic Communications Regulations
USA FEDERAL
CALEA, CCRA, CIPA, COPPA, EFTA, FACTA, ECPA, FCRA, FISMA, FERPA, GLBA, HIPAA, HITECH, PPA, RFPA, Safe Harbor, US PATRIOT Act
CANADA
PIPEDA, FOIPPA, PIPA
EUROPEAN UNION
EU Data Protection Directive, Sate Data Protection Laws
SOUTH KOREA
Network Utilization and Data Protection Act
JAPAN
Personal Information Protection Act
US STATES
Breach notification in 46 states
MOROCCO
Data Protection Act
ISRAEL
Protection of Privacy Law (PPL)
THAILAND
Official Information Act B.E. 2540
TAIWAN
Computer-Processed Personal Data Protection
MEXICO
Personal Data Protection Law
INDIA
Information Technology Act
HONG KONG
Personal Data Privacy Ordinance
BRAZIL
Article 5 of Constitution
COLOMBIA
Data Privacy Law 1266
SINGAPORE
Personal and Financial Data Protection Acts
PHILIPPINES
Propose Data Privacy Law
ARGENTINA
Protection of Personal Data Act, Information Confidentiality Law
SOUTH AFRICA
Electronic Communications and Transactions Act
CHILE
Protection of Personal Data Act
AUSTRALIA
National Privacy Principals, State Privacy Bills, Email Spam and Privacy Bills
NEW ZELAND
Privacy Amendment Act

Figure 3. Applied laws for Cloud Data depending on the host country

As can be seen in Figure 3, in worldwide terms beside Germany, the USA present one of the most restrictive jurisdictions about legal concerns regarding sensitive Cloud Data protection. In the area of federal security and privacy regulation for healthcare, the first related legislation, called electronic protected health information (ePHI), was specified in 1996 as a part of the Health Insurance Portability and Accountability Act (HIPAA) (Wu, 2007). HIPAA legislation includes, among others, the following aspects (Herold & Beaver, 2004):

- Enhancement of patients' rights by providing them with access to their medical records.
- Protection of patients' rights by controlling access to their records.
- Improvement of the efficiency and effectiveness of healthcare delivery and data exchange.
- Reduction of healthcare costs.

The security regulations concerned with electronic medical information were published by the Department of Health and Human Services as The Security Rules in 2002 (Choi, Capitan, Krause, & Streeper, 2006). The regulations require appropriate administrative, physical, and technical protection methods to ensure ePHI integrity, confidentiality, and security ("Health Information Privacy," n.d.).

Sanctions by failure to comply with federal HIPAA regulations can end in fines of up to $1.5 million and up to 10 years in prison. The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and

Reinvestment Act of 2009, is also relevant because it has several provisions that strengthen the civil and criminal enforcement of the HIPAA rules, mainly by defining levels of culpability and corresponding penalties (*Health Information Technology for Economic and Clinical Health (HITECH)*, 2009) These penalties are intended to force ePHI owners to take privacy and security concerns very seriously. The Security Rule contains broad and complex implementation specifications, and guidelines that relate to security administration (conducting risk analyses and implementing policies and procedures to address vulnerabilities, assigning responsibility and developing incident response plans among other measures), technical safeguards (activity audits, encryption, user identity management, data integrity verification) and physical safeguards (protecting and limiting access to servers, storage media, and workstations). So movement of electronic health records among applications and outside the healthcare establishment's corporate perimeter involves implementation of many of the HIPAA-required security processes and technologies by the cloud provider.

But clinical datasets are not the only law regulated information. Countries like Spain have developed legislations such as Organic Law 15/1999 for Protection of Personal Data (1999) and governmental agencies (AEPD, *Agencia Española de Protección de Datos*) to ensure compliance with the law. The following types of data are considered as personal and have to be secured accordingly:

- **Sensitive data**: Ideology, union affiliation, religion, beliefs, racial or ethnic origin, health and sex life.
- **Identification data**: ID, address, image, voice, Social Security Number, phone number, physical marks, name, signature / fingerprint, digital signature, health card.
- **Data on personal characteristics**: marital status data, family data, date of birth, place of birth, age, sex, nationality, native language and physical or anthropometric characteristics.
- **Data relating to social circumstances**: accommodation features, housing, family status, property, possessions, hobbies and lifestyles, clubs and associations memberships, licenses, permits and authorizations.
- **Academic and Professional Data**: Training, qualifications, student history, professional experience, professional bodies or associations' memberships.
- **Job Details**: Job, economic data, worker history.
- **Business related Information**: activities, business, subscriptions to publications and media, artistic, literary, scientific or technical creations.
- **Economic, financial and insurance data**: Income, investments, capital assets, credits, loans, guarantees, bank details, pension plans, retirement, financial payroll data, tax data/taxes, insurance deductions, mortgage subsidies, benefits, credit history, credit cards.
- **Data relating to transactions in goods and services**: Goods and services provided by the affected goods and services received by the affected financial transactions, compensation / damages.

Sanctions established by failure to comply with this legislation are classified in three different levels, from minor to very severe, incurring in fines from 900€ up to 600.000€.

In summary, the assessment of legal regulations shows, that all person-related data (and particularly medical data, sensitive or critical data) in CC and other outsourcing scenarios should be protected from access by the service provider or other unauthorized third parties. In general, the different laws stipulate only global requirements. The definition and implementation of specific measures is the obligation of the specific organization. For example, it should apply general measures for protecting personal data (e.g. limited access) also with respect to health-related data and it can further extend them with measures to protect data transmission (e.g. encryption).

4.4.2 Elaboration

The elaboration of the framework concerning the legal environment deals specifically with legal regulations in Germany for the particularly challenging area of healthcare providers. The proposed elaboration has been published by the author in a special issue of IT Professional regarding IT governance in healthcare (Dzombeta et al., 2014).

Almost every institution within the healthcare system— from general practitioners' offices to hospitals to medical insurance companies—must process personal patient data, including sensitive aspects of the patient's health status. In Germany, there is a wide range of applicable regulations that govern the protection of individual rights and the "informational self-determination rights" of patients. The universally applicable Federal Data Protection Act or *Bundesdatenschutzgesetz* (BDSG; http://tinyurl.com/7uayj6r) defines health data as a special type of personal data with legally mandated increased protection requirements (section 3, paragraph 9 of the law.) The collection, processing, and use of health data is generally allowed only for the purposes of preventive medicine and medical diagnosis, care, or treatment, or for the purpose of managing and administering health services. Such data can be processed only by medical personnel or by other people who possess the same appropriate confidentiality obligations (section 28, paragraph 7 of BDSG).

Regarding specifying and meeting such requirements, several aspects emerge – the contract between involved parties (for example in outsourcing environments) should specify the type and scope of the intended data use, the client's control rights (such as the right to conduct independent audits on the premises of the service provider), as well as specific technological and organizational measures that the provider will implement to comply with technical and organizational requirements.

The client thus must be careful when selecting the service provider, ensuring that the provider is capable of taking the appropriate technological and organizational measures. This obligation to verify that the provider is taking the appropriate measure is known as the "control obligation," and it can be fulfilled in person or using experts, information security management system auditors, self-disclosure forms from the provider, as well as certificates or proofs of established data protection concepts from the provider. If the client fails to comply with this control obligation, the government or independent regulatory bodies can fine the client.

The obligation further continues during the actual data processing through regularly controls. The frequency of such follow-up verifications differs in accordance with the scope of data processing, the associated risks, the innovation cycle of related technologies, as well as the type of the processed data. Relevant cloud computing providers in Germany conduct yearly audits implemented by independent organizations and make the audit reports available to their clients.

Compared to these general requirements of data processing under a mandate by an outsourcing provider, the specific case of processing social data is regulated similarly but by a different law (section 80 of SGB X). There are several important differences between section 80 of SGB X and section 11 of BDSG that need to be considered.

According to SGB X, client organizations are expected to use only providers from the public administration. A client can only use a private cloud computing provider if using a public provider will cause substantial problems to normal operations or if the private provider offers substantial cost benefits (both of which would be difficult to assess and verify formally).

The provider location is also highly relevant in this regard. When considering data processing under a mandate as stipulated by section 11 of BDSG, organizations in the life sciences should ensure that the cloud computing providers process data exclusively within the EU or the European Economic Area (EEA). Due to the EEA-wide harmonization of data protection regulations in Directive 95/46/EC (especially considering current efforts to further increase levels of protection), cloud computing providers from the EU are expected to meet EU criteria even if they operate outside of the EU.15 Nevertheless, this work recommends that when drafting contracts with providers that operate outside of the EU, clients should specify that data processing outside the EU/EEA is not allowed.

Cloud computing providers located outside countries and jurisdictions of the EU/EEA cannot conduct data processing under a mandate as stipulated by section 11 of BDSG. From the viewpoint of BDSG, data processing in such jurisdictions is considered data transmission, which requires specific authorization. Determining whether such transmission can be authorized is conducted in two steps.

First, it should be assessed whether the specific country already exhibits a proper data protection level (section 2(2), paragraph 4b of BDSG). The EU Commission itself conducts such assessments based on international treaties and has currently found proper levels for only a handful of countries, including Argentina, Australia, Guernsey, and Canada. The US is currently not among these countries, but based on US-EU Safe Harbor Framework (now followed by the EU-U.S. Privacy Shield Framework), certain certified providers are considered safe. If the general level of data protection isn't considered appropriate, data transmission can only be contractually specified using the preformulated EU standard contract clauses in verbatim. Furthermore, because these clauses only partially cover the requirements of BDSG, this work also recommends that the requirements of section 11, paragraph 2 of BDSG be additionally covered in the contract.

Second, in addition to ensuring the appropriate data protection level of the country where the provider processes the data, the organization still needs a legal foundation for data transmission in a country outside the EU/EEA. The case of health-related data is specifically regulated in section 28, paragraphs 6–9, of BDSG. Transmission of a person's data without explicit consent is possible under extremely limited conditions. For example, the processing of such data can only be conducted by people who are subject to the medical confidentiality requirement. This will be the case only if the provider is considered a so called "accomplice" ("*Gehilfe*" in German), which is a professionally active assistant of the doctor as defined in section 203, part 3 of the Criminal Code or *Strafgesetzbuch* (StGB; www.iuscomp.org/gla/statutes/StGB.htm#203), which is not usually the case with a typical client-provider relationship.

When considering the already presented legal aspects and inherent risks of cloud-based data processing for organizations in the areas of healthcare and life sciences, it's evident that the organizations should define their requirements with respect to data privacy. The definitions should consider aspects such as the selection and evaluation process of possible cloud computing providers, specific detailed requirements about service-level agreements (SLAs), as well as specifically required organizational and technical measures to which the cloud computing provider should conform. This dramatically increases transaction costs in the cloud computing market, which is already marked by high levels of information asymmetry (Stantchev & Tamm, 2012).

Some existing automated approaches for matching demand and supply, even for the SLA phase (Stantchev & Tamm, 2011) are only of limited benefit, because they cannot account properly for complex organizational measures. However, specific technical measures can be clearly stated in automated supply statements (for example, the service level objectives) and can therefore be easily matched to automated requirements.

Recommendations for specific measures can be derived from generally applicable standards, such as ISO 27001 and ISO 29100 (see www.iso.org). These can serve as a framework for managing information security and protecting data within the context of cloud computing and other outsourcing relationships. Additionally specific standards like ISO/IEC 27018:2014: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors or the Baseline IT-Security or IT-*Grundschutz* standard by the Federal Office for Information Security or *Bundesamt für Informationssicherheit* (BSI; https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html) offer additional control specifications. They provide specific controls to assist the user in achieving the objectives like how to select the proper cryptographic method, manage security keys and how to configure encryption modules reliably for cloud environments.

The already discussed, preformulated EU standard contract clauses should be incorporated verbatim into the service contract. Significant attention should be paid to the detailed description of technical and organizational measures, because these constitute the contractually agreed upon security concept.

The client organization serving the life sciences or healthcare fields should also consider continuity management in particular, because emergency and failover scenarios often lead to substantial security breaches. The volatility and frequent changes in the cloud computing market require detailed specifications about the proper and adequate handling of data in the case of the outsourcing contract's termination.

The sheer amount and diversity of the data protection requirements means that an integral part of organization-wide information security management systems must be the governance of cloud computing and outsourcing relationships. Therefore, in this thesis a detailed approach for assessing the legal environment is presented.

The approach considers four general phases and thus can be easily applied not only as part of the proposed holistic framework, but also in the context of most IT governance approaches (Stantchev & Stantcheva, 2012). The four phases of the approach are:

- plan,
- select a cloud computing provider,
- negotiate contractual specified delivery mechanisms, and
- monitor and govern operation.

Table 2 gives a detailed view of the questions that need to be answered in order to gain an as complete as possible input to the proposed compliance framework from the legal environment.

4.4.3 Questionnaire

The artefact that was developed as a result of the elaboration in the area of legal environment is a questionnaire. This questionnaire is intended to serve as a method for soliciting, categorizing, merging and structuring the relevant legal aspects so that they can be developed to reliable and stable requirements within the framework.

Table 2. The proposed Questionnaire for soliciting Input from Legal Environment

#	Question
1.	Which data is affected by the outsourcing decision? Higher risk data such health-related, social, or medically confidential?
2.	Which legal frameworks are applicable?
3.	Which existing risks are associated with the outsourcing decision: data availability, confidentiality, or integrity?
4.	Which requirements exist concerning data protection: appropriate security architecture, data encryption and cryptography, identity and rights management, control possibilities, monitoring and security incident management, contingency plans and measures, and others?
5.	Which barriers are present? No data storage outside the EU or European Economic Area (EEA), or outside some other area?
6.	Is the provider compliant with legal and data protection requirements?
7.	Where does the provider store data (EU/EEA or other jurisdiction)? If other, does an appropriate protection level exist? If the US, is the provider Safe Harbor certified? If corporate structures of the provider reside outside the EU (for example, internal providers residing outside EU), how are they involved in the data processing?
8.	Does the provider have an information security management system (ISMS) concept?
9.	How was the ISMS concept assessed concerning appropriateness of technical and organizational measures and how is the result of the assessment documented?
10.	Does the provider have current and internationally established certifications (for example, ISO 27001)?
11.	Is the cloud computing service precisely and clearly formulated?
12.	Are appropriate control rights for the cloud user organization and corresponding obligations for the cloud provider being specified?
13.	Are there clauses that govern the contingency operation and the return of data in the case of bankruptcy of the cloud provider?
14.	Is there a mandate for data processing?
15.	When operating in non-EU jurisdictions, are the EU standard clauses or Binding Corporate Rules part of the agreement?
16.	Are there specific, relevant service-level agreements? Do they outline the availability and dependability requirements, response and restoration deadlines, computing power, and support details?
17.	Are there specific contingency regulations for the case of catastrophic failures?
18.	Are controls being conducted regularly? Are there assessments of the agreed-upon technical and organizational measures?

19.	Are the security concepts being regularly assessed? Are they current, and do they correspond to the current state of the art?

4.4.4 Qualitative Study

As already stated, for the purpose of the qualitative study of robustness of the developed artefact the following application of NGT was conducted.

The NGT assessment was conducted with a group of seven experts. The insights that they developed inside the assessment were as follows:

1. During the phase of silent generation, the experts were presented with the questionnaire for the *legal environment*. The *Nominal Question* they had to address was "Is the questionnaire sound and robust enough to gather all relevant compliance aspects for the relevant subject matter (*legal environment*)? Provide 3-5 reasons for your opinion!" All expert provided opinions that assessed the questionnaire as sound and robust enough with reasons provided such as "It covers all relevant sources of legal requirements for an organization in Germany.", "It corresponds to best practices I have witnessed before.", and "It is structured from common to specific and is also multi-dimensional."
2. During the round-robin feedback phase, the experts explained their reasons to the others and the reasons were recorded on a whiteboard.
3. During the group clarification phase, the experts conducted a structured group discussion that established three main reasons – a) "The structure of the questionnaire is well aligned", b) "The questionnaire allows to assess the relevant sources for legal requirements for a specific organization", and c) "The questionnaire accounts for the important dimensions of such assessment – location, sector, type of data".
4. During the individual voting and ranking on priority of ideas phase, experts voted and ranked the reasons.
5. During the final phase – discussion of group consensus results and focus on potential next steps – the experts reached a consensus to rank the reasons as follows:
   a) "The questionnaire accounts for the important dimensions of such assessment – location, sector, type of data", b) "The questionnaire allows to assess the relevant sources for legal requirements for a specific organization", and c) "The structure of the questionnaire is well aligned".

The conducted NGT-based qualitative study provided a clear signal that the developed artefact for this subject domain – *the questionnaire for the legal environment* – is sound and robust enough to be assessed as part of the framework in the following phases of this thesis.

4.5 Organizational and processual environments

In the following, the relevance and the state-of-the-art approaches in the area of assessing legal environment will be discussed and subsequently elaborated. Then, the relevant framework element – *organizational and processual environments* – will be elaborated and the relevant artefact from the framework will be developed. At the end, NGT approach will be applied within a qualitative study to decide whether the artefact is robust enough.

4.5.1 Assessment of Relevance and Related Approaches

Cloud Computing is directly based on Service Oriented Architecture (SOA). Following SOA, a service in the Cloud Computing environment can be a piece of software (Software as a Service, SaaS), a platform (Platform as a Service, PaaS) or a part of the infrastructure (Infrastructure as a Service, IaaS) (Chazalet, 2010b), see also Figure 4. The goal of cloud computing is to optimize the usage of physical and software resources, improve flexibility and automate management, which reduce costs and increase revenue for cloud service providers (Chan & Chieu, 2010; Chazalet, 2010a).

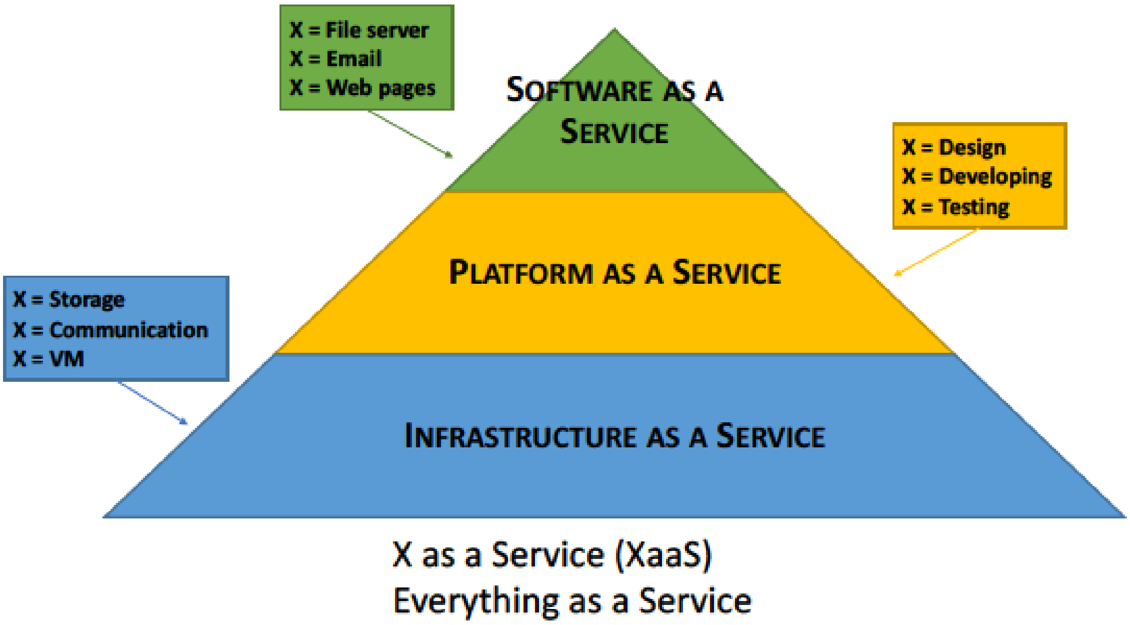


Figure 4. Overview of Layers in Cloud Computing and the Cloud Services provided at each level

In organizational and processual environments, it is fundamental to consider governance. In this case, Cloud Computing governance can be based on SOA governance due to its direct correspondence. As defined by IBM (IBM, 2006), SOA governance is an extension of IT governance, which is an extension of corporate governance. SOA Governance exercises control of the lifecycle of services and composite applications in an organization's Service-Oriented Architecture (SOA). Its main functions are:

- Establish decision rights for the development, deployment, operations and management of new services.
- Monitor and report decisions and results for communicating governance results.

SOA Governance provides the Business/IT alignment needed to achieve the SOA promise-of-value for service reuse and improved business agility. The two key components of SOA Governance are Service Governance (Brown, 2009) and Organizational Change (Mills, 2007). These two dimensions reflect closely the challenge of the framework in this subject domain – to present a unified view of both structural aspects (organizational hierarchy and rules of coordination) and dynamic aspects (provided internal and external services).

4.5.2 Elaboration

SOA governance can facilitate an agile, fast, effective decision making across both business and IT, and enhance the ability to rapidly build, configure and assemble services to form innovative solutions in the marketplace, reducing bureaucratic obstacles that get in the way. Also, it can speed resolution when things do not work according to the plan, as involved people will understand who to go to and how best to resolve issues for maximum effectiveness. This knowledge can help speed change, enabling organizations to react more quickly and decisively to competitive threats and marketplace opportunities. Finally, acceptance of and agreement on services that provide the greatest value encourages adoption and reuse of those services and reduces wasted effort and cost.

The adopted model for SOA Governance in the proposed Compliance Framework is based in the one proposed in (Schröpfer, 2010), shown in Figure 5.

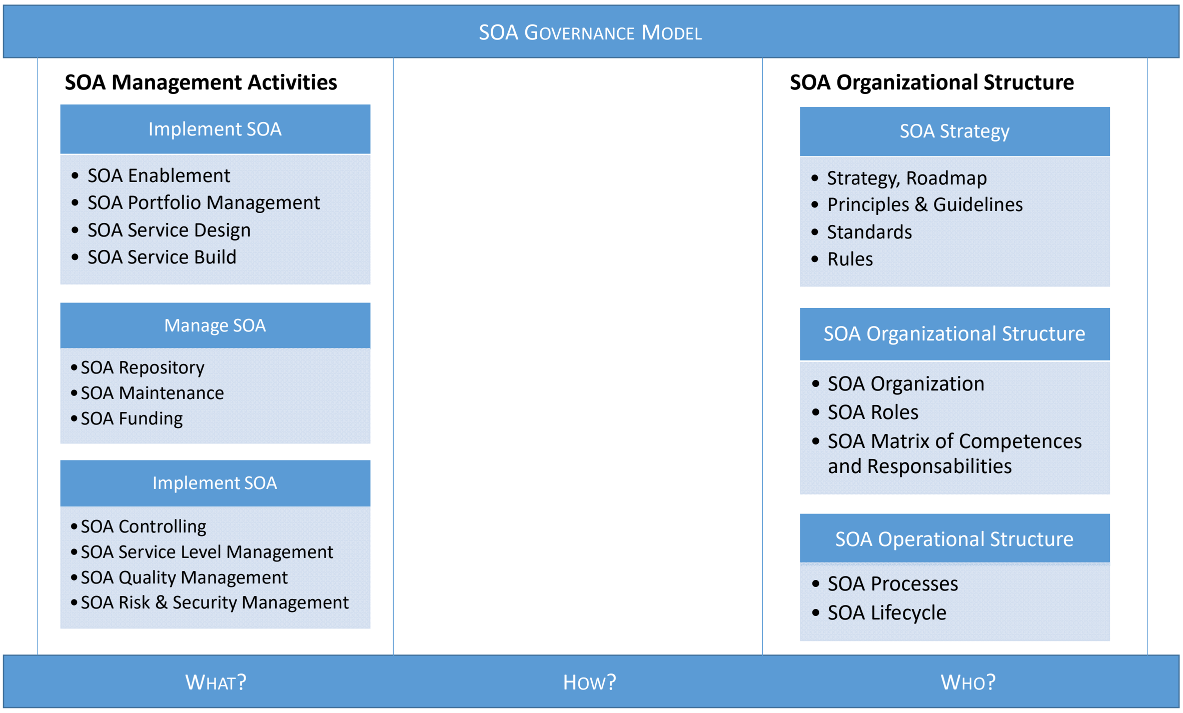


Figure 5. General overview of Shelp & Stutz's SOA-Governance-Model

This model is not a complete framework, but it has a scientific basis, and it represents well the different interconnections among elements and roles. This helps to have a general overview of how governance should be applied in an efficient way.

The process by which business and IT solutions such as CC are brought in line with each other to enhance the performance of business and to achieve business goals is called strategic alignment (Mekawy, Rusu, & Ahmed, 2009). The proposed compliance framework considers inputs from SOA Strategy and Operations, following the Henderson and Venkatraman's Strategic Alignment Model (SAM), (Henderson & Venkatraman, 1993) which is perhaps the most widely cited of all alignment models. Another key model is the one developed by Jerry Luftman to assess the maturity of this IT/Business alignment (Luftman, 2003; Luftman, Lyytinen, & Zvi, 2015; Luftman, Papp, & Brier, 1999). In any case, the topic is an important topic in Information Systems research (Bartens, Schulte, & Voß, 2014; J. Choi, Nazareth, & Jain, 2013; Dahlberg, Hokkanen, & Newman, 2016; Gerow, Grover, Thatcher, & Roth, 2014; Kaidalova, Siegerroth, Bukowska, & Shilov, 2014; Pereira, Silva, & Lapão, 2014; Siurdyban, 2012; Wagner, Beimborn, & Weitzel, 2014; Yaokumah, Brown, & Adjei, 2015; Yayla & Hu, 2011).

The SAM model is based on four related key domains of strategic choice, namely business strategy, organizational infrastructure and processes, IT strategy, and IT infrastructure and processes (see Figure 6). In the SAM model, the concept of strategic alignment is distinct from bivariate fit (i.e., linking only two domains) and cross-domain alignment (i.e., linking any three domains). A distinction is also drawn between the external perspective of IT (IT strategy) and the internal focus of IT (IT infrastructure and processes). The potential of IT to both support and shape business policy is recognized (Henderson & Venkatraman, 1992).

The SAM model has received empirical support and has substantial conceptual and practical value (Avison, Jones, Powell, & Wilson, 2004).

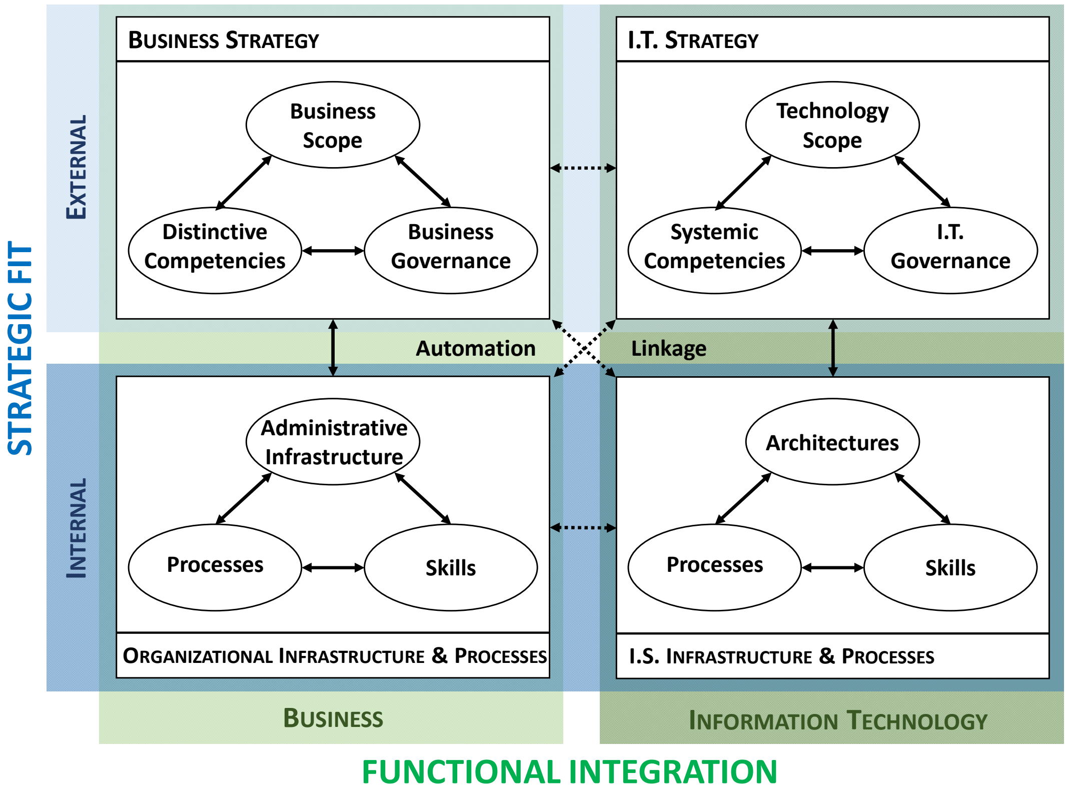


Figure 6. The Henderson and Venkatraman Strategic Alignment Model

This combined approach of SOA Governance and business – IT alignment provides a vantage point to define questions that reflect not only general and isolated insights about organization, processes or IT. The incorporation of SOA Governance allows to solicit specific governance problems that are typical when using CC. Furthermore, the incorporation of SAM paradigms allows to account for challenges in business – IT alignment specifically, and not only focus on IT aspects. Moreover, while SAM considers business – IT alignment in a more top-level manner, its combination with the SOA Governance approach aims to allow the proposed framework to achieve a level of precision and detail that is not typical for business – IT alignment.

In order to assess this section of the framework, a qualitative study involving experts in the area of SOA governance, and strategy alignment will be planned and conducted to check the validity of proposed hypothesis.

4.5.3 Questionnaire

The questionnaire aims to combine paradigms from SOA Governance and business – IT alignment in an approach to solicit the relevant input in the specific subject field (organizational and processual) for the purpose of risk assessment and compliance assurance of the framework. In addition, further questions and considerations are possible. The questionnaire can be also applied within tailored comprehensive surveys, as they have been shown to be a good evaluation mechanism (Mekawy et al., 2009).

Table 3. The proposed Questionnaire for soliciting Input from Organizational and Processual Environment

#	Question
1.	Are there existing guidelines for the introduction of changes in processes and in process steps? What are the effects of such changes on other processes? What are the effects of such changes on the corporate strategy? Is it assured that security aspects are to be considered during the introduction of changes? Are all changes planned, tested, approved and documented? Are fallback solutions developed before the implementation of changes? Is the information security management involved in all substantial changes?
2.	Are enterprise-critical processes affected? How about the data availability in these processes? Effects on the availability of other processes?
3.	Are there changes in the responsibilities and roles resulting from the change?
4.	Emergency Plan Assessment of the documentation of latest emergency tests Security concept Routine security assessments at the CSP and other contractors by certified third party Authentication, authorization, administration, audits, awareness access control Data processing is allowed solely according to the instructions of the cloud user, no data usage by the CSP for own purposes Penetration tests at the CSP and other contractors Monitoring by the cloud user should be possible, SLA fulfilment should be provable Logging and monitoring of administrator activities Four-eyes-principle during critical administration activities Provision of logfiles by the CSP Information about security incidents 24/7 response team for Security Incident Handling and Trouble Shooting 24/7 Monitoring of cloud services and an immediate response to security incidents Implementation of proper measures against internal threats that are inherent in a multi-tenant architecture Establishment of transparency and trust by the provision of detailed information intended for the cloud user Measures at the personnel level Police certificate

	Educational history, qualifications, current and past affiliations Personal environment (e.g. party membership) Courses in IT security Courses in social engineering Control and education for awareness Assessment of contractors (e.g., technicians, facility managers) Data security and non-disclosure agreements

4.5.4 Qualitative Study

Here again, for the purpose of the qualitative study of robustness of the developed artefact the following application of NGT was conducted.

The NGT assessment was conducted with a group of six experts. The insights that they developed inside the assessment were as follows:

1. During the phase of silent generation, the experts were presented with the questionnaire for the *organizational and processual environment*. The *Nominal Question* they had to address was "Is the questionnaire sound and robust enough to gather all relevant compliance aspects for the relevant subject matter (*organizational and processual environment*)? Provide 3-5 reasons for your opinion!" All expert provided opinions that assessed the questionnaire as sound and robust enough with reasons provided such as "It solicits input from most relevant stakeholders.", "It corresponds to state-of-the-art approaches in the area of system analysis and process improvement.", and "It reflects typical challenges of organizations."
2. During the round-robin feedback phase, the experts explained their reasons to the others and the reasons were recorded on a whiteboard.
3. During the group clarification phase, the experts conducted a structured group discussion that established three main reasons – a) "The structure of the questionnaire reflects its objectives", b) "The questionnaire allows to assess the relevant sources for organizational and processual requirements for a specific organization", and c) "The questionnaire provides a tool that combines both organizational (structure) and processual (dynamics) aspects".
4. During the individual voting and ranking on priority of ideas phase, experts voted and ranked the reasons.
5. During the final phase – discussion of group consensus results and focus on potential next steps – the experts reached a consensus to rank the reasons as follows:
   a) "The questionnaire provides a tool that combines both organizational (structure) and processual (dynamics) aspects", b) "The questionnaire allows to assess the relevant sources for organizational and processual requirements for a specific organization", and c) "The structure of the questionnaire reflects its objectives".

The conducted NGT-based qualitative study provided a clear signal that the developed artefact for this subject domain – *the questionnaire for the organizational and processual environment* – is sound and robust enough to be assessed as part of the framework in the following phases of this thesis.

4.6 Technological Environment

In the following, the relevance and the state-of-the-art approaches in the area of assessing legal environment will be discussed and subsequently elaborated. Then, the relevant framework element – *technological environment* – will be elaborated and the relevant artefact from the framework will be developed. At the end, NGT approach will be applied within a qualitative study to decide whether the artefact is robust enough.

4.6.1 Assessment of Relevance and Related Approaches

Today, in most developed societies, information technologies have become pervasive. This is information technologies are in fact used throughout society. The development of sophisticated Web technologies has brought about a fundamental shift in types of information technologies that are being used; whereas traditionally each user would install applications for various tasks (from creating documents to playing digital media) on the computer, Web technologies enable using the Internet as the platform for applications. Now, much of the functionality previously offered by applications installed on a computer is offered by applications hosted and executed by cloud environments (Valacich, Schneider, & Jessup, 2014).

In addition to changing the way people work and interact, information technology has also enabled *globalization*, the integration of economies throughout the World, fundamentally changing how not only people but also organizations and countries interact.

In this globalized market, is required for organizations to adapt their procedures to work as a "learning organization". A learning organization is one that is "*skilled at creating, acquiring, and transferring knowledge, and at modifying its behaviour to reflect new knowledge and insights*" (Garvin, 2000). Being a learning organization allows to take competitive advantage over competitors by refining internal strategies and gaining differentiation due the increased knowledge at different layers.

An organization has competitive advantage whenever it has an edge over rivals in attracting customers and defending against competitive forces (Porter, 2001; Porter & Millar, 1985). Some sources of competitive advantage include the following:

- Having the best-made product on the market
- Delivering superior customer service
- Achieving lower costs than competitors
- Having a proprietary manufacturing technology, formula, or algorithm
- Having shorter lead times in developing and testing new products
- Having a well-known brand name and reputation
- Giving customers more value for their money

Companies and organizations can gain or sustain each of these sources of competitive advantage by effectively using information systems. Executives today who are serious about using information technology in innovative ways have made it a point to have their people be continually on the lookout for new disruptive innovations that will have a significant impact on their business.

4.6.2 Elaboration

Wheeler has summarized the process of considering technological developments and incorporating them as part of your organization and business model nicely as the e-business innovation cycle (Wheeler, 2002) (see Figure 7). Like the term "e-commerce," "e-business" refers to the use of information technologies and systems to support the business. Whereas "e-commerce" generally means the use of the Internet and related technologies to support commerce, e-business has a broader meaning: the use of nearly any information technologies or systems to support every part of the business. The model essentially holds that the key to success for modern organizations is the extent to which they use information technologies and systems in timely, innovative ways. The vertical dimension of the e-business innovation cycle shows the extent to which an organization derives value from a particular information technology, and the horizontal dimension shows the passage of time.

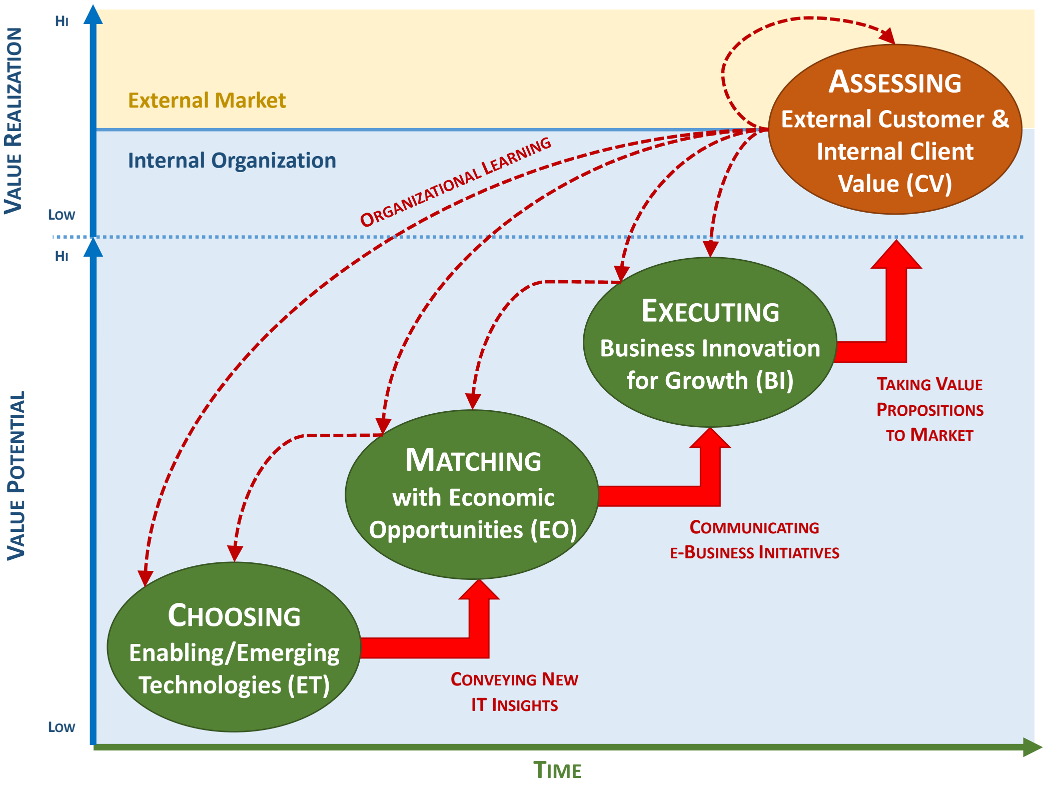

VALUE REALIZATION
HI
LOW
VALUE POTENTIAL
HI
LOW
External Market
Internal Organization
ORGANIZATIONAL LEARNING
ASSESSING
External Customer & Internal Client Value (CV)
EXECUTING
Business Innovation for Growth (BI)
MATCHING
with Economic Opportunities (EO)
CHOOSING
Enabling/Emerging Technologies (ET)
TAKING VALUE PROPOSITIONS TO MARKET
COMMUNICATING E-BUSINESS INITIATIVES
CONVEYING NEW IT INSIGHTS
TIME

Figure 7. Wheeler's E-Business Innovation cycle

The first bubble bottom left of the graph (Choosing enabling/emerging technologies) shows that successful organizations first create jobs, groups, and processes oriented to scanning the environment for new emerging and enabling technologies (i.e., information technologies that enable a firm to accomplish a task or goal or to gain or sustain competitive advantage in some way. This is, disruptive innovations) that appear to be relevant for the organization.

Next, in the second bubble (Matching with economic opportunities), the organization matches the most promising new technologies with current economic opportunities (such as advances in database management systems and a dramatic drop in data storage costs).

The third bubble (Executing business innovation for growth) represents the process of selecting the appropriate technologies/advances and then addressing the current opportunity to grab customers and market share.

The fourth bubble (Assessing external customer & internal client value) represents the process of assessing the value of that use of technology, not only to customers but also to internal clients (i.e., sales representatives, marketing managers, the chief operating officer, and so on).

The proposed questionnaire for soliciting requirements in this subject field of the compliance framework will base its fact-finding process implementation in the technology environment by means of using the Wheeler's e-business innovation cycle, together with specific aspects derived from technology acceptance assessment approaches such as the Technology Acceptance Model (TAM), see Figure 8. TAM models in general how 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 a person believes that using a particular system would be free from effort*) (Davis, 1989).

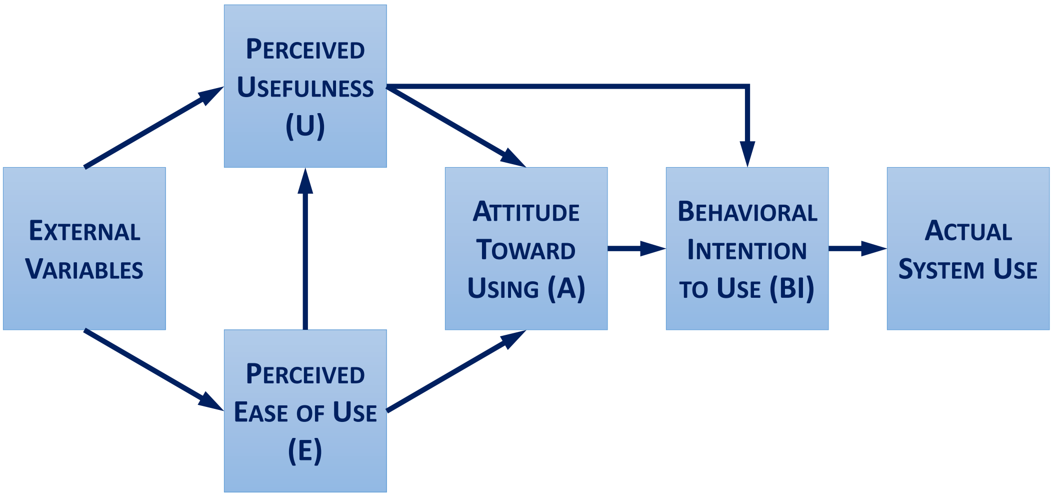

Perceived Usefulness (U)
External Variables
Attitude Toward Using (A)
Behavioral Intention to Use (BI)
Actual System Use
Perceived Ease of Use (E)

Figure 8. Technology Acceptance Model (TAM)

TAM is based on the Theory of Reasoned Action (TRA) developed by (Ajzen & Fishbein, 1980). The TRA theorizes that the intention to accept or reject a particular technology is based on a series of trade-offs between the perceived benefits of the system to the user and the difficulty of learning or using the given system. The TRA suggests that conduct results from the formation of specific intentions to behave. According to this model, two major factors determine behavioural intentions namely: user attitude toward the behaviour and subjective norms. Attitude toward the behaviour refers to the person's judgment that performing the behaviour is good or bad. The subjective norms reflect the person's perception of social pressures put on him/her to perform or not the behaviour in question. In line with the theory, attitudes are a function of beliefs. In this sense, a person who believes that performing a given behaviour will lead to positive outcomes will hold a positive attitude toward performing the behaviour.

The TAM is devoted to identifying barriers and enablers to the adoption of new technologies in a particular setting. The model suggests that perceived usefulness, defined as “the degree to which an individual believes that using a particular system would enhance his or her productivity”, and perceived ease of use, defined as “the degree to which an individual believes that using a particular system would be free of effort”, are key determinants of the actual usage of a particular technology or system (Davis, 1989). This tool has been widely cited as a research artefact in the information systems arena in a variety of fields and scenarios e.g. (Broman Toft, Schuitema, & Thøgersen, 2014; Cheung & Vogel, 2013; Joo & Sang, 2013; Padilla-Meléndez, del Aguila-Obra, & Garrido-Moreno, 2013; Park, Baek, Ohm, & Chang, 2014; Park & Kim, 2014; Stantchev, Colomo-Palacios, Soto-Acosta, & Misra, 2014; Svendsen, Johnsen, Almås-Sørensen, & Vittersø, 2013; Wallace & Sheetz, 2014).

4.6.3 Questionnaire

This following questionnaire is proposed as the mean to solicit input in the specific subject field (technological). The questionnaire aims to combine paradigms from technology innovation (e-business innovation cycle) and technology assessment (TAM) in an approach to solicit the relevant input in the specific subject field (technological). In the same time, it maintains a focus on the specific purpose of risk assessment and compliance assurance in change management in CC as being the objectives of the framework.

Table 4. The proposed Questionnaire for soliciting Input from Technological Environment

#	Question
1.	What technologies are available for user and access management, role-based access control, two factor authentication?
2.	What technologies are available for encryption during data processing and data transport?
3.	What technologies are available for data backup, restoration and availability of the service?
4.	What technologies are available for redundant supply of power, HVAC, water?
5.	What technologies are available for fire protection?
6.	What technologies are available for robust infrastructure, redundant network connection, emergency working places etc.?
7.	What technologies are available for redundant data centres, documentation and control of availability management?
8.	What technologies are available for building security, access control, and secure entry area?
9.	What technologies are available for control of service contractors (cleaning, facility management, repair technicians)?
10.	What technologies are available in the area of server security? - Host protection (firewall, intrusion detection, integrity checking) - Secure standard configuration (beefed-up operating system)

	- Sandbox for every virtual machine - Certified hypervisors (at least CC EAL4, IT SEC E3) - Redundant images / services of the provided - A secure sandbox environment in the case of IaaS in order to prevent exploits on host systems - Assessment of system documentation, status, log files
11.	What technologies are available in the area of network security? - Redundant network links - Safeguards against attacks, malware - Secure configuration of all cloud components, network segmentation - Encrypted remote administration - Encrypted communication between CSP and cloud user - Encrypted communication between different CC sites - Encrypted communication to and from third party contractors - Encrypted transmission of network management information - Analysis of VPN infrastructure and end-to-end encryption chain
12.	What technologies are available in the area of application and platform security? - Integration of security management into the software life cycle, security gates, vulnerability tests, audits, etc. - Application isolation, interface monitoring - Automatic monitoring and assessment of user applications - Patch and change management, patch compatibility tests - Control whether guidelines von development of secure applications are applied
13.	What technologies are available in the area of information security? - Patch and change management - Definition of life cycle of customer data - Secure isolation - Role-based information access, e.g. based on LDAP - Regular backups (extent, intervals, storage concept, times and durations) - Complete and secure deletion - Every component can be targeted by an attach, therefore analysis of weaknesses and protection measures (end-to-end security)
14.	What technologies are available in the area of encryption and key management? - Only assured and secure encryption methods are used - Random generated keys with sufficient length - Secure asynchronous key exchange - Short duration of keys, secure storage of keys - Key destruction, e.g. utilizing SAML - Strong authentication of cloud users (two-factor authentication)
15.	What technologies are available for overcoming the lack of standardization in CC? - The customer should ensure if the provider uses standardized technology and it should be mentioned in its initial contract. - Hybrid cloud approaches to avoid compatibility issues between cloud and IT systems in customer's organization

4.6.4 Qualitative Study

As already stated, for the purpose of the qualitative study of robustness of the developed artefact the following application of NGT was conducted.

The NGT assessment was conducted with a group of seven experts. The insights that they developed inside the assessment were as follows:

1. During the phase of silent generation, the experts were presented with the questionnaire for the *technological environment*. The *Nominal Question* they had to address was "Is the questionnaire sound and robust enough to gather all relevant compliance aspects for the relevant subject matter (*technological environment*)? Provide 3-5 reasons for your opinion!" All expert provided opinions that assessed the questionnaire as sound and robust enough with reasons provided such as "It accounts for relevant technologies.", "It corresponds to best practices I have witnessed before.", and "It aims for a view that reflects both what innovation aspects technology can provide and how they contribute to compliance assurance."
2. During the round-robin feedback phase, the experts explained their reasons to the others and the reasons were recorded on a whiteboard.
3. During the group clarification phase, the experts conducted a structured group discussion that established three main reasons – a) "The structure of the questionnaire is well aligned", b) "The questionnaire allows to solicit technological requirements of a specific organization", and c) "The questionnaire accounts for both technology potentials and compliance needs".
4. During the individual voting and ranking on priority of ideas phase, experts voted and ranked the reasons.
5. During the final phase – discussion of group consensus results and focus on potential next steps – the experts reached a consensus to rank the reasons as follows:
   – a) "The questionnaire allows to solicit technological requirements of a specific organization", b) "The structure of the questionnaire is well aligned", and c) "The questionnaire accounts for both technology potentials and compliance needs".

The conducted NGT-based qualitative study provided a clear signal that the developed artefact for this subject domain – *the questionnaire for the technological environment* – is sound and robust enough to be assessed as part of the framework in the following phases of this thesis.

4.7 Cultural Environment

In the following, the relevance and the state-of-the-art approaches in the area of assessing legal environment will be discussed and subsequently elaborated. Then, the relevant framework element – *cultural environment* – will be elaborated and the relevant artefact from the framework will be developed. At the end, NGT approach will be applied within a qualitative study to decide whether the artefact is robust enough to be subjected to an evaluation as part of the framework.

4.7.1 Assessment of Relevance and Related Approaches

National and even regional cultures do matter for management (Hofstede, 1983b). The national and regional differences are concerns for empirical research. In fact, these differences may become one of the most crucial problems for management – in particular for the management of multinational, multicultural organizations, whether public or private. For the purpose of this Ph.D. thesis, the definition of (Hofstede, Hofstede, & Minkov, 2010) will be adopted. The definition is as follows: "Culture is the collective programming of the human mind that distinguishes the members of one human group from those of another". This author also provided strong evidence that national cultural differences shape organizational behaviour at a local level, and that differences in national and regional cultures affect work values (Hofstede, 2003). Thus, organizations around the globe need to create a common corporate culture in their commercial relationships or develop cultural competence among their workers. As described by this author, national culture is important to management for at least 3 reasons:

- **Political**. Nations are political units with their own institutions (forms of government, educational systems, legal systems, labour and employer's association systems). Not only do the formal institutions differ, but the informal ways of using them differ.
- **Sociological**. Nationality or regionality has a symbolic value to citizens due to the identity feeling. The symbolic value of the fact of belonging to a nation or region has been and still is sufficient reason for people to go to war, when they feel their common identity to be threatened.
- **Psychological**. Citizens thinking is partly conditioned by national culture factors. This is an effect of early life experiences in the family and later educational experiences in schools and organizations, which are not the same across national borders.

However, there are other models devoted to study national culture. Social scientists have conducted wide-ranging research on how cultures differ and the dimensions to compare those (Olson & Olson, 2003). Apart from the model developed by Hofstede, two major models have analysed culture dimensions in the literature: (Hall, 1977) and (Trompenaars & Hampden-Turner, 2012) model. The three present comparable features and have been discussed widely in the literature (Casado-Lumbreras, Colomo-Palacios, Gomez-Berbis, & Garcia-Crespo, 2009; Casado-Lumbreras, Colomo-Palacios, Soto-Acosta, & Misra, 2011). However, it is important to note that the model developed by Hofstede focuses on the values and culture of computer professionals. As a consequence, the model have been widely utilized within information systems research e.g. (Casado-Lumbreras, Colomo-Palacios, Ogwueleka, & Misra, 2014; Casado-Lumbreras, Colomo-Palacios, Soto-Acosta, et al., 2011; Choi, Im, & Hofstede, 2016; Hovav & D'Arcy, 2012; Myers & Tan, 2002; Ruano-Mayoral, Casado-Lumbreras, Garbarino-Alberti, & Misra, 2014; Sundararajan, Bhasi, & Pramod, 2017; Wiedenhöft, Luciano, & Testa, 2015; Zhang, de Pablos, & Xu, 2014) and, therefore, deserves our consideration for the purposes of this work.

Further in his research, Hofstede defines a set of dimensions (or different criteria) to classify national cultures among a large set of countries through a combination of multivariate statistics (factor analysis) and theoretical reasoning. The defined cultural dimensions are:

- **Power Distance**. The fundamental issue involved is how society deals with the fact that people are unequal in physical and intellectual capacities. In organizations, the level of Power Distance is related to the degree of centralization of authority and the degree of autocratic leadership. A culture with high power distance is characterized by an established hierarchy of power, based on status, wealth, intellectual capacity, or some other factors. Inequality is here considered a law of nature, rather than a problem. On the contrary, a culture with low power distance considers every individual as equal, despite differences in power, status or wealth.
- **Individualism vs. Collectivism**. The fundamental issue involved is the relation between an individual and his or her fellow individuals. In some cultures is more important to look after self-interest and maybe the interest of immediate family, while in others there exist a big concept of tribe (from extended family to village). The collectivist's preference is to be part of a community. These people are expected to give loyalty to the groups they belong to. Unlike, in an individualistic culture, the interest of the individual prevails over that of the group. The ties between individuals are loose. Every person is considered as an independent entity capable of making his/her own decisions, and is expected to be fully responsible for the consequences.
- **Uncertainty Avoidance.** The fundamental issue involved here is how society deals with the fact that future is unknown as well as the events that can happen. Some societies socialize their members into accepting this uncertainty and not becoming upset by it; they are societies in which people have a natural tendency to feel relatively secure. On the contrary, other societies socialize their people into trying to beat the future; they are societies in which people develop a higher level of anxiety, nervousness, emotionality and aggressiveness. This kind of societies create the security feeling by means of technology, laws, rules and institutions, nomination of experts (people assume them to be beyond uncertainty) and religion.
- **Masculinity vs. Femininity**. This dimension intends to find out whether an organization (or a society) minimizes gender role differences and gender discrimination. Men are supposed to be assertive, strong and focused on material success, while women are gentle, caring and concerned with quality of life.

- **Long-term vs. Short-term Time Orientation**. This dimension shows to what degree people value the future versus the past or the present. Values associated with long term orientation are thrift and perseverance, whereas values associated with short term orientation are respect for tradition, fulfilling social obligations, and protecting one's 'face'.
- **Indulgence vs. Restraint**. Indulgence stands for a society that allows relatively free gratification of basic and natural human drives related to enjoying life and having fun. Restraint stands for a society that suppresses gratification of needs and regulates it by means of strict social norms.

The naive assumption that management is the same or is becoming the same around the world is not tenable in view of these demonstrated differences in national cultures. It should be adapted depending on the country and culture. According to Hofstede study, the most relevant dimensions for leadership are Individualism and Power Distance. In organizations the decisive dimensions of culture are Power Distance and Uncertainty Avoidance, and the practices of motivating people can both be related to the Individualism-Collectivism dimension.

4.7.2 Elaboration

Kluckhohn and Strodtbeck proposed the existence of a limited set of questions, called "cultural orientations", which each society must answer to operate in an effective and cooperative way, and a limited set of possible answers for each question, called "variations". The development of the theory, guided in part by Parsons, Shils and Smelser's general theory of action (Parsons, Shils, & Smelser, 1965), took place over 10 years through rigorous content analysis of a generation's worth of field studies from around the World. This led to the Cultural Orientations Framework (Kluckhohn & Strodtbeck, 1961). In this scheme, culture is defined as the pattern of variations within a society, or, more specifically, as the pattern of deep-level values and assumptions associated with societal effectiveness, shared by an interacting group of people. Kluckhohn and Strodtbeck and their research associates identified a set of six basic cultural orientations with two or three possible variations each. The six value orientations answer the following specific questions:

- What is the nature of human beings: are they good, evil or neutral?
- What is our relationship to nature: are we subjugated to nature, in harmony with nature, or do we have mastery over it?
- What is our relationship to other human beings: is it lineal (ordered position within groups), collateral (primacy given to goals and welfare of groups), or individualistic (primacy given to the individual)?
- What is our primary mode of activity: is our basic orientation one of being-in becoming, doing or reflecting?
- How do we view time: do we focus on the past, present, or future?
- How do we think about space: is it public, private, or mixed?

The framework has been proven to be valid by some studies, such as (Connolly & Lang, 2012; Maznevski, Gomez, DiStefano, Noorderhaven, & Wu, 2002), in which authors present empirical data gathered from five countries (Canada, Mexico, the Netherlands, Taiwan, and the United States) and contrast the results of the framework with the cultural dimensions defined by Hofstede.

Cloud Computing environments are thought to be used worldwide, among different nations and cultures. In the same time, cultural aspects strongly influence risk and compliance considerations. Therefore, the relevant artefact of the proposed compliance framework must consider the different cultural environments and their differences. As an initial approach, the Cultural Orientations Framework and the cultural dimensions defined by Hofstede will be taken into account to define an appropriate set of questions the answers to which can help to homogenise the compliance process among these different cultures.

4.7.3 Questionnaire

This following questionnaire is proposed as the mean to solicit input in the specific subject field (cultural). The questionnaire aims to combine paradigms from the Cultural Orientations Framework and the cultural dimensions defined by Hofstede in an approach to solicit the relevant input in the specific subject field (cultural). In the same time, it maintains a focus on the specific purpose of risk assessment and compliance assurance in change management in CC as being the objectives of the overall framework.

Table 5. The proposed Questionnaire for soliciting Input from Cultural Environment

#	Question
1.	What are the countries of incorporation of headquarters, main offices and branches of the organization?
2.	What are the countries of incorporation of main accounts of the organization?
3.	What market reach does the organization have (regional, national, international, and world-wide?
4.	What other predominant cultural aspects exist (e.g. a religious or non-profit organization)?
5.	What are the relevant cultural dimensions (according to Hofstede and subsequent works) for the organization?
6.	Which metrics about the relevant cultural dimensions are needed?
7.	How are needed metrics about the relevant cultural dimensions accumulated?
8.	What is the relevance of every relevant cultural dimension for the change management?
9.	How are the relevant metrics considered during the change process?

4.7.4 Qualitative Study

Following the approach from the previously presented subject areas, as a qualitative study of robustness of the developed artefact (questionnaire for soliciting input from cultural environment) the following application of NGT was conducted.

The NGT assessment was conducted with a group of five experts. The insights that they developed inside the assessment were as follows:

1. During the phase of silent generation, the experts were presented with the questionnaire for the *cultural environment*. The *Nominal Question* they had to address was "Is the questionnaire sound and robust enough to gather all relevant compliance aspects for the relevant subject matter (*cultural environment*)? Provide 3-5 reasons for your opinion!" All expert provided opinions that assessed the questionnaire as sound and robust enough with reasons provided such as "It reflects the most commonly used cultural dimensions.", "It corresponds to best practices I have witnessed before.", and "It considers relevant metrics, too."
2. During the round-robin feedback phase, the experts explained their reasons to the others and the reasons were recorded on a whiteboard.
3. During the group clarification phase, the experts conducted a structured group discussion that established two main reasons – a) "The structure of the questionnaire is well aligned to solicit relevant cultural dimensions", and b) "The questionnaire allows to assess existing and applicable metrics".
4. During the individual voting and ranking on priority of ideas phase, experts voted and ranked the reasons.
5. During the final phase – discussion of group consensus results and focus on potential next steps – the experts reached a consensus to rank the reasons as follows:
   a) "The structure of the questionnaire is well aligned to solicit relevant cultural dimensions", and b) "The questionnaire allows to assess existing and applicable metrics".

The conducted NGT-based qualitative study provided a clear signal that the developed artefact for this subject domain – *the questionnaire for the cultural environment* – is sound and robust enough to be assessed as part of the framework in the following phases of this thesis.

4.8 The Inner Works

Previous sections included artefacts for the first four components, now the artefact that is in charge of the actual change management process needs to be incepted. The particular focus lies in the aggregation of the inputs and their digestion to structured actions that reflect the objectives of risk assessment, change management and compliance in CC.

CC, due to its elastic nature, reduces initial investments as it can create servers on demand. It is flexible, scalable, on demand service and portable to any device. It is designed to be accessed anytime and anywhere through the wired and wireless networks including the Internet. This wide set of features increase the number of possible risks to affect a cloud environment. A study by Dutta et al (Dutta, Peng, & Choudhary, 2013) identified several cloud computing risks perceived by IT experts which are classified around operational, organizational, technical, and legal areas (thus reflecting pretty well the subject domains of the proposed framework). The identified risks include issues in preparation and planning which relate to the deficiencies of CC. Furthermore, emerging recent works tend to consider information security for CC through the prism of established governance frameworks (Rebollo et al., 2015) which is also the approach chosen in this work.

Frameworks with comparable objectives are proposed by some major cloud vendors (e.g., the IBM whitepaper "Defining a framework for cloud adoption"[4]). Furthermore, there are some holistic approaches to address cloud usage or adoption currently emerging in the research landscape. The Cloud Computing Business Framework (Chang, Walters, & Wills, 2013) suggests an approach that is structured in the areas of Classification (here cloud service providers are classified), Organisational Sustainability Modelling (here a requirements analysis is performed), Service Portability (deals with service migration), and Linkage (deals with linking services together in a process chain). Another recent development is the proposal of a Cloud computing adoption framework with focus on security aspects (Chang et al., 2016). It is a security-oriented framework oriented towards first adoption of cloud services and suggests a layered approach to security. Suggested layers are: firewall, identity management and encryption. Yet another framework – this one aimed towards ranking of cloud services – was presented by Garg et. al. (Garg, Versteeg, & Buyya, 2013). It considers QoS aspects such as accountability, agility, assurance of service, cost, performance, security and privacy in order to provide a service measurement index (SMI).

An approach that aims to combine CC and outsourcing was also presented recently (Yongsiriwit, Assy, & Gaaloul, 2016). The authors follow the paradigm of Business Process as a Service (BPaaS) and considers semantic representations in order to allow for functional mapping between internal and outsourced processes.

Furthermore, there are practical approaches that aim to incorporate standard information security and compliance certification frameworks into the topic of compliance of CC, with one of the most complete requirement catalogues published in March 2016 by the German Federal Authority for Information Security

[4] http://www-935.ibm.com/services/us/cio/itxpo/4_defining-a-framework-for-cloud-adoptionciw03067usen.pdf

(*Bundesamt für Informationssicherheit*, BSI)[5]. In its reference part[6] it provides a mapping of its requirements to the requirements of several certification standards – ISO/IEC 27001:2013(Chaudhuri, 2015), CSA Cloud Control Matrix 3.01(Chaudhuri, 2015), AICPA Trust Services Principle Criteria 2014[7] and others.

While all these approaches exhibit some similarity in areas of coverage and employed paradigms, there are still important gaps and shortcomings that remain to be addressed – particularly with respect to change management during an ongoing usage of cloud services.

The proposed Compliance Framework for Change Management in Cloud Environments (CFC MCC) relies on an established change management process. It is assumed that an adequate and well-conducted change management process usually has at least the following activities:

- initiating, documenting and authorize changes
- assessment of the impacts, costs, benefits and risks of changes under consideration
- justification and approval of changes
- plan and coordinate the implementation of changes
- monitoring and reporting on the implementation
- Review and finalization of Request for Changes (RFCs)

Figure 9, based on the works by (Taylor, Lacy, & Macfarlane, 2011) shows a generic change management process, which is based on ITIL v3 (Van Bon et al., 2010). This process is taken as the reference model for the further elaboration of the actual change management process within the proposed framework.

[5] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/Anforderungskatalog.html

[6] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/Anforderungskatalog_Referenzierung.html

[7] http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/tspc/exposure_draft/ed_tsp_principles.pdf; https://www.ssi.gouv.fr/actualite/appel-public-a-commentaires-sur-le-referentiel-dexigences-applicables-aux-prestataires-de-services-securises-dinformatique-en-nuage/ ; https://www.idw.de/idw/idw-aktuell/idw-ers-fait-5-zu-den-gob-bei-it-outsourcing-einschliesslich-cloud-computing/27514 ; https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/IT-Grundschutz_14_Ergaenzungslieferung_veroeffentlicht_19122015.html ; https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Sicherheitsprofile/sicherheitsprofil_saas_node.html

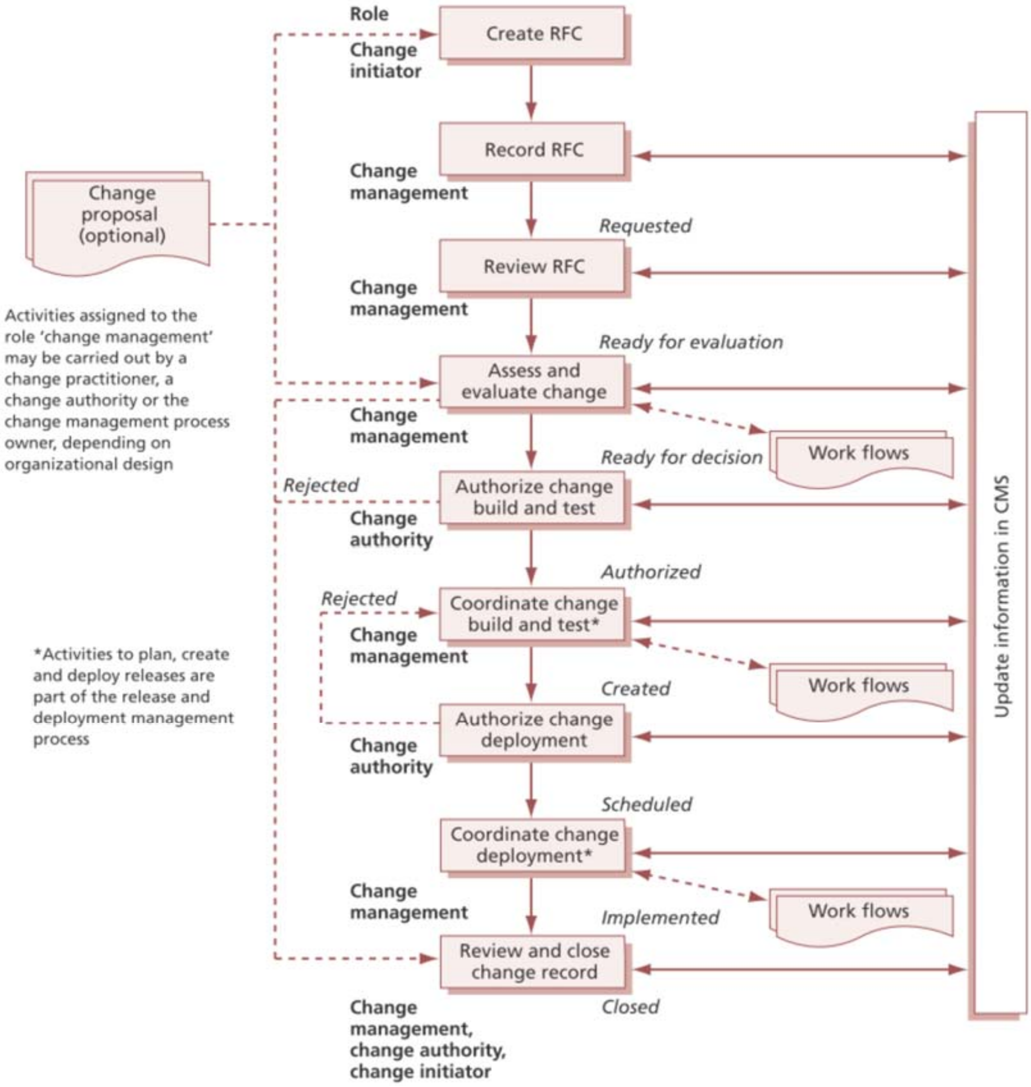

Role
Create RFC
Change initiator
Record RFC
Change management
Change proposal (optional)
Requested
Review RFC
Change management
Activities assigned to the role 'change management' may be carried out by a change practitioner, a change authority or the change management process owner, depending on organizational design
Ready for evaluation
Assess and evaluate change
Change management
Ready for decision
Work flows
Rejected
Authorize change build and test
Change authority
Authorized
Rejected
Coordinate change build and test*
Change management
*Activities to plan, create and deploy releases are part of the release and deployment management process
Work flows
Created
Authorize change deployment
Change authority
Scheduled
Coordinate change deployment*
Change management
Work flows
Implemented
Review and close change record
Change management, change authority, change initiator
Closed
Update information in CMS

Figure 9. A Standard Change Management Process in ITIL V3

There are several reasons why an elaboration of a new change management process is not pursued in the context of the proposed framework. First, the focus of the framework lies in the introduction of governance-specific aspects in a change management process, not in the definition of a completely new change management process. Furthermore, the effects of CC and hybrid cloud scenarios are to be considered as well. Thus, the cornerstone is to provide a path to introduce a Cloud Governance view (Dzombeta et al., 2014) with focus on security and compliance as an extension of organizational change management. Also, when considering the maturity of the topic of change management it is evident that it is one of the most mature parts of IT governance frameworks (Sharifi, Ayat, Rahman, & Sahibudin, 2008).

Objectives of the change management process are to detect changes, to document them, to comply with the necessary permits and oversee the implementation.

Furthermore, it ensures that changes are scheduled, executed efficiently, cost-effectively and with controlled risk (Taylor et al., 2011).

According to the ITIL definition the following reasons for changes, for example, are possible (Taylor et al., 2011):

- New or updated hardware or network components
- New or updated application software
- New or updated system software, including patches and bug fixes
- change in legislation, or the conformity with the guidelines
- Business need
- improvement of processes, procedures and / or underlying tools
- Changes in the management or staff
- Changes to the service level or service delivery

The aim of the proposed framework is to find a smart approach to respond to similar emergent changes in cloud environments effectively and efficiently by relying on an already established change management process.

A well-established and mature change management process of an organization with traditional IT-Governance often does not cover all the necessary compliance considerations that are associated with a transition to a CC environment. An assessment of the impact of such transition on the organizational compliance is rarely conducted or is considered mostly an afterthought. As a result, compliance risks associated with such a transition and the resulting changes are often identified very late in the transition process or even not at all. Consequently, the costs of risk management are significantly higher.

4.8.1 Definition Process of the Framework

The CFC MCC focuses on a risk-based analysis of the changes in the CC and is based on the input from the subject-matter questionnaires that were presented in the previous sections. This corresponds to the step "assess and evaluate change" in the change management process according to ITIL v3. Therefore, it is aimed at allowing a straightforward risk assessment of the planned changes associated with the transition to or the subsequent usage of the cloud environment. Classical change management processes such as ITIL do not address all potential issues specified in the sections above and do not consider all relevant risks or requirements regarding usage of CC.

The inner works of CFC MCC encompass the following steps (see Figure 10):

1. Identification of the important information and processes as primary organizational assets
2. Identification of secondary assets for the association with measures (inheritance)

3. Definition of protection requirements for considered information in CC and of gross risk based on potential damage and likelihood
4. Current status: Already existing measures
5. Risk evaluation after existing measures and of considered change (net risk)
6. Remaining steps and new measures / controls

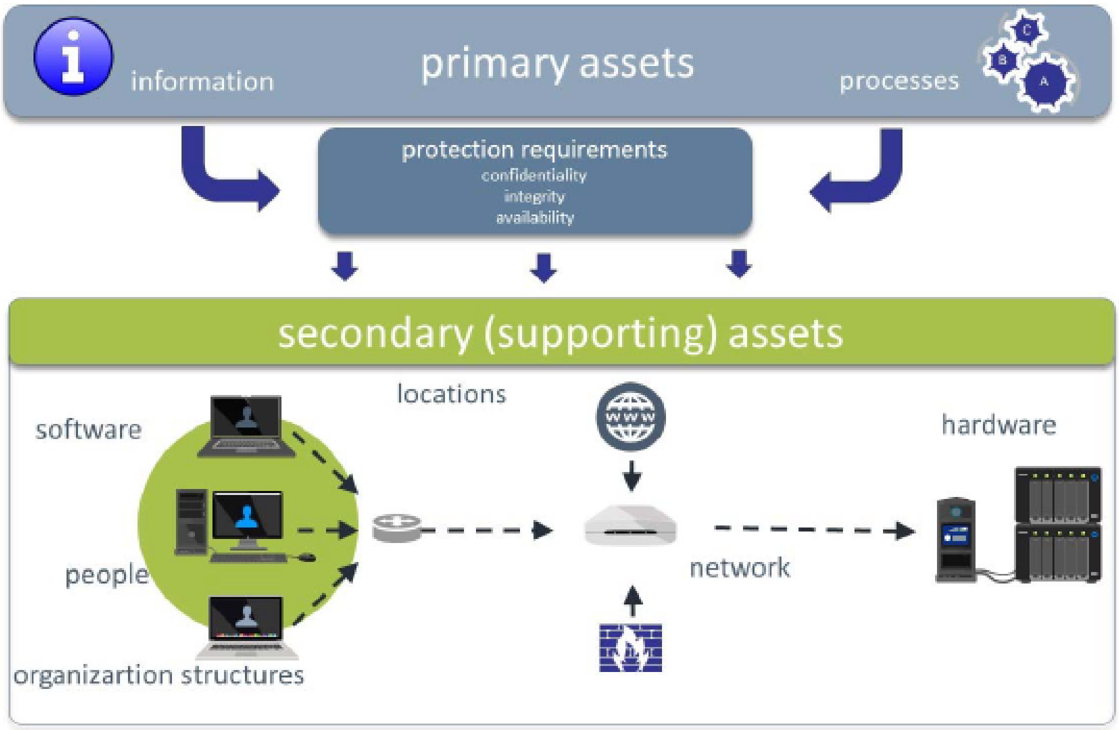


Figure 10. An Architectural Overview of the Inner Works of CFC MCC

The last step to defining measures is not considered further in this work as defining measures and KPIs is not the primarily focus of the framework itself. For this the framework will rely on existing common standards - for example, oriented to the Cloud Controls Matrix[i] or the Capability Maturity Model Integrated (CMMI Product Team, 2010). Such standards will also be used within the validation of the framework.

4.8.2 Definition of Protection Requirements Categories

The goal of defining the protection requirements is to decide for the affected data in CC which protection requirements the data has in terms of confidentiality, integrity and availability. These protection requirements are based on the potential damage which comes in conjunction with the impairment of the affected applications and therefore of the corresponding business processes.

There are various approaches for security requirements elicitation. Some focus on reuse (Toval, Nicolás, Moros, & García, 2002) while others consider misuse and breaches (Sindre & Opdahl, 2005).

The first step is to define the protection requirement categories with typical categories. After defining the protection requirements categories, the protection requirements for considered data have to be defined based on the typical damage scenarios. Part if this consideration is also the assessment of secondary assets like IT systems, rooms, and communication interfaces etc.

Since the protection requirements are usually not easily quantifiable, we divide the protection requirements into three qualitative categories as shown in the following table.

Table 6. Proposed Protection Requirements Categories

protection requirements categories	Values
low	The impact of any loss or damage is limited and calculable.
medium	The impact of any loss or damage may be considerable.
high	The impact of any loss or damage may be of catastrophic proportions which could threaten the very survival of the organization.

The following steps describe how to determine the appropriate protection requirements category for the considered data having in mind the relevant business processes and their underlying applications.

The damage that could occur if the confidentiality, integrity, or availability is lost for a particular business process or application, including its data, can usually be categorized according to the following damage areas:

- legal: Violations of laws, regulations, or contracts, Impairment of the right to informational self-determination
- organizational/ processual: Impaired ability to perform the tasks at hand, Impairment of business processes or activities, Physical injury
- technical: elimination of a specific technology from the approved assets list due to compromised security
- cultural: - negative internal or external effects, cultural misunderstandings
- Financial consequences

All these categories (apart from the “financial” category which is a generic one) correspond to the categories defined as subject field areas of the proposed framework in the previous sections.

It is often the case that several damage scenarios will apply to a single damage event (Stantchev, Colomo-Palacios, & Niedermayer, 2014). For example, the failure of an application could prevent essential business activities from being performed, resulting in direct financial loss and in negative reputation.

In order to differentiate between the "low", "medium", and "high" protection requirements categories, it may be appropriate to determine the limits of each damage scenario. The following tables are used to determine the protection requirements resulting from a potential damage scenario and its consequences. Each organization must adapt the tables to reflect its own situation.

Table 7. Decision Support for Defining Requirements Categories per Topic Area

areas / category	low	medium	high
legal	• Violations of regulations and laws with minor consequences • Minor breaches of contract which result in at most minor contractual penalties • This deals with personal data which processing could adversely affect the social standing or financial wellbeing of those concerned.	• Violations of regulations and laws with substantial consequences • Major breaches of contract with high contractual penalties • This aspect deals with personal data whose processing could have a seriously adverse effect on the social standing or financial well-being of those concerned.	• Fundamental violations of regulations and laws • Breaches of contract with ruinous damage liabilities • This aspect deals with personal data which processing could result in the injury or death of the persons concerned or that could endanger the personal freedom of the persons concerned.
organizational / processual	• Impairment was assessed to be tolerable by those concerned • no or little impact on business objectives, customers or business partners	• Impairment of the ability to perform the tasks at hand was assessed as intolerable by some of the individuals concerned. • one or more business	• Impairment of the ability to perform tasks was assessed as intolerable by all individuals concerned. • one or more major business objectives will not be achieved long-

areas / category	low	medium	high
	• No or short-term impairment of critical processes. The maximum acceptable downtime is greater than 24hours. • Physical injury does not appear possible	objectives will not be achieved negative impact on customers and business partners • long-term impairment of relevant processes; The maximum acceptable down time is between one and 24 hours. • Physical injury to an individual cannot be absolutely ruled out.	term negative impact on customers and business partners • long-term value of the company massively disrupted; The maximum acceptable down time is less than one hour. • Serious injury to an individual is possible. There is a danger to life and limb.
technical	• no critical infrastructure or technology affected • no major vulnerabilities of standard infrastructural assets involved • no technological details of specific competitive advantage revealed	• a single critical infrastructure or technology affected • a single vulnerability of a standard infrastructural asset involved • minor technological details of specific competitive advantage revealed	• multiple critical infrastructures or technologies affected • multiple vulnerabilities of standard infrastructural assets involved • major technological details of specific competitive advantage revealed
cultural	• no or little effect on cultural mindset in the organization • no or little effect on cultural mindset of customer base • no or little effect on cultural mindset in the organizational environment	• expected negative impact in 1-2 relevant dimensions of the cultural mindset in the organization • expected negative impact in 1-2 relevant dimensions of the cultural mindset of customer base • expected negative impact in 1-2	• expected negative impact in more than two relevant dimensions of the cultural mindset in the organization • expected negative impact in in more than two relevant dimensions of the cultural mindset of customer base • expected negative impact in in more

areas / category	low	medium	high
		relevant dimensions of the cultural mind-set in the organizational environment	than two relevant dimensions of the cultural mindset in the organizational environment
financial	• The financial loss is considerable, but does not threaten the existence of the organization. • >Amounts to be defined<	• The financial loss is considerable, but does not threaten the existence of the organization. • >Amounts to be defined<	• The financial loss threatens the existence of the organization. • >Amounts to be defined<

In the next step the protection requirements are inherited to the secondary assets. Dependencies exist between the different assets that affect the classification to a certain degree. The following rules should apply to the inheritance:

Maximum rule: The maximum rule defines that the classification of a resource is defined be the highest requirement category of a process that uses this resource or a piece of information that is processed by this resource.

Accumulation: Accumulation effects occur always when multiple not so important resources are depending on a single resource and the sum of these resources or the affection of integrity, confidentiality of availability causes a higher damage (higher classification) than the affection of a single resource. Accumulation is to be applied at the distinct resources starting at the level of applications.

Distribution: The distribution effect is the opposite of the accumulation effect. It occurs when the application area of a resource is distributed over multiple other resources. The classification of the corresponding resource can then be lowered. Distribution is to be applied at the distinct resources starting at the level of applications.

In effect, both the primary and the secondary assets have then their own specific protection requirements.

4.8.3 Process Steps and Examples

4.8.3.1 Protection Areas, Gross Risk without Measures/Controls

First the data affected by CC transition and the associated substantial assets need to be determined. Assets here refer to so called secondary assets, which support the business processes and other activities. One example is the corresponding IT infrastructure.

Following this scope identification is the definition of the protection requirements. This can in general be done according to established methods such as reuse (Toval et al., 2002) or considering misuse and breaches (Sindre & Opdahl, 2005). Nevertheless, for the purpose of the proposed framework it is mandatory to start with a fresh assessment, without considering existing governance instruments or security measures. The classification of the requirements is done according to the specified areas (legal, organizational/processual, technical and cultural) and categories. The questionnaires that were presented in the previous sections serve as an elicitation tool for the requirements.

Next, the potential damage should be identified, the likelihood of occurrence is to be estimated. Both serve as a basis for the calculation of the gross risk.

The result of the protection requirements (column 4) is calculated by the maximum principal (the maximum of the separate protection requirement categories).

The following Table 8 is showing one example.

Table 8. Example for Defining Requirements Categories per Topic Area

1. scope	2. Requirements	3. protection area	4. protection requirement categories				5. result	6. potential damage	7. likelihood	8. gross risk
data/asset	Reference		legal	oraganizational/ processual	technical	cutural	effects considered	max. financial	in %	result risk analysis
test data	„References to specific requirements“	Confidentiality	h	m	l	l	h	150 T€	10%	15 T€
		Integrity	h	m	l	l	h			
		Availability	h	m	l	l	h			

The risks of not complying with requirements are identified and weighted – this is the gross risk calculation (column 8). Already established measures are not considered during this. So the risk potential is calculated by multiplying the potential damage (column 6) with the likelihood of occurrence (column 7). Each organization defines thresholds of significance (ToS) for the gross risk calculation.

The calculated gross risk can be regarded as part of IT risk management. This allows the utilization of various management instruments. One example is the risk matrix that can be used to document gross risk is presented in what follows.

Table 9. A Risk Matrix as an Example for Documentation of Gross Risk (ToS – Threshold of Significance)

Likelihood of occurrence	Very high	>50%	🟨	🟥	🟥
	high	> 20%-<50%	🟩	🟨	🟥
	medium	5% - 20%	🟩	🟨	🟥
	low	< 5%	🟩	🟨	🟨
	Finaicial loss		<=ToS	1-5 x ToS	> 5 x ToS
	Reputation damage		low	medium	high
	Regulatory damage				
	Potential damage				

Using this type of risk matrix, it is possible to assess the effectiveness of existing measures and whether there is a need to introduce changes to their current status.

4.8.3.2 Existing Measures and Current Status

After defining the protection requirements and the gross risk, all already implemented measures or controls should be considered. This step is merely a documentation step and serves as an additional input for the subsequent steps.

The following table is showing one example.

Table 10. Example for Documenting Existing Control Measures per Topic Area

scope	existing measure/control	current status	date

data/asset	measure/control	technical	organizational/ processual	sufficient	realization status	
test data	A	x		y		
	B		X	n	ongonig	2015
	...	x		y		

4.8.3.3 Net Risk after First Implemented Measures and Considered Change

The following activity of the framework is now a second assessment of (security) requirements and a derived calculation of the net risk after first implemented measures. The assessment of security requirements now requires two steps:

1. Reduction of the already documented (security) requirements in order to account for the already introduced measures and controls.
2. Further calibration of requirements based on the planed transition of data to CC. This can again lead to a new increase in the number or category of requirements.

Furthermore, this can lead to a decrease or increase of the potential damage and/ or a change in the likelihood of occurrence. Thus, the net risk needs to be calculated.

In order to improve clarity, an organization can conduct these two steps sequentially and document them separately. In this case it should calculate net risk (based on existing implemented measures) and an additional net risk II – based on the risk assessment of the planned change.

The following table is showing one example:

scope	protection requirement categories (after control implementation)				result	potential damage (after control implementation)	likelihood (after control implementation)	Net risk
data/asset	legal	oraganizatio	technical	cutural		max. financial	in %	
test data	m	m	m	m	m	100.000€	5%	5.000€

	m	m	m	m	m			
	m	m	m	m	m			

Table 11. Example for Documenting Gross Risk

4.8.3.4 Reaming Steps Initiated by Change

The last step includes the definition of new measures and assurance of a proper risk level during the implementation of the change in CC. As already mentioned, in this case measures from existing standards such as the Cloud Controls Matrix can be considered.

Table 12. Example for Defining Measures for Change Management in CC

scope	remaining steps	possible measures/controls					implementation		date	
data/asset		measure/control	technical	organizational/processual	expenses	effectiveness approved	ongoing	finished and approved		comments
test data										

4.8.4 Qualitative Study

Following the approach from the assessment of the first four artefacts of the framework (the questionnaires for soliciting relevant inputs from the legal, organizational and processual, technological, and cultural environments) a qualitative study of robustness of the final developed artefact (the inner works) through the following application of NGT was conducted.

The NGT assessment was conducted with a group of seven experts. The insights that they developed inside the assessment were as follows:

1. During the phase of silent generation, the experts were presented with the abbreviated description of the process described in this section (*the inner*

works). The *Nominal Question* they had to address was "Is the approach sound and robust enough to achieve the stated goals of the framework? Provide 3-5 reasons for your opinion!" All expert provided opinions that assessed the approach as sound and robust enough with reasons provided such as "The approach can serve as the foundation of compliance-oriented change management.", "It corresponds to best practices I have witnessed before.", and "It is structured to reflect typical organizational concerns and objectives."

2. During the round-robin feedback phase, the experts explained their reasons to the others and the reasons were recorded on a whiteboard.
3. During the group clarification phase, the experts conducted a structured group discussion that established three main reasons – a) "The approach can be established as an extension to an existing change management process in an organization", b) "The approach allows to quantify impact of changes on compliance", and c) "The approach builds on both the inputs from the previously developed artefacts and on the existing change management process".
4. During the individual voting and ranking on priority of ideas phase, experts voted and ranked the reasons.
5. During the final phase – discussion of group consensus results and focus on potential next steps – the experts reached a consensus to rank the reasons as follows:

   a) "The approach can be established as an extension to an existing change management process in an organization", b) "The approach allows to quantify impact of changes on compliance", and c) "The approach builds on both the inputs from the previously developed artefacts and on the existing change management process".

The conducted NGT-based qualitative study provided a clear signal that the developed artefact – *the inner works* – is sound and robust enough to be assessed as part of the framework in the following phases of this thesis. Together with the qualitative studies performed for all other framework elements, this makes the framework mature enough to transition to the next phases of assessment in the following chapters.

4.9 Summary of the Framework

The presented Compliance Framework for Change Management in Cloud Environments (or CFC MCC) aims to provide a compliant change management in the context of CC. This is achieved by first soliciting relevant input from the defined subject fields – legal, organizational and processual, technological, and cultural. For each subject field a specific artefact (questionnaire) was developed, that serves as a mean to solicit and structure the inputs to proper requirements. Subsequently, the robustness of all these artefacts was assessed by qualitative studies following the NGT technique.

The structured inputs are then processed in the so called *Inner Works* of the framework – a compliance-oriented and risk-aware change management approach that extends best practices in change management to provide a compliant approach for handling CC-related changes. More specifically, the approach assesses specific risks associated with changes related to CC and results in specific suggestions for risk- and compliance-enhancing measures that should be implemented along with the original CC-related change. This area of the framework was also subjected to an assessment in a qualitative study based on the NGT and the study assessed this artefact also as robust enough. The subsequent industry cases that will be presented within the evaluation will provide specific examples of such measures.

The structuring of subject fields on the "outskirts" and a process that "crunches" input in a multistage process to provide specific measures corresponds to approaches that were proposed recently for application in industry[8]. A specific example is the requirement catalogue published in March 2016 by the German Federal Authority for Information Security (*Bundesamt für Informationssicherheit*, BSI)[9]. Published during the final stages of the thesis – when the framework was already developed and validated – during its evaluation stage, the catalogue confirms most of the paradigms that the framework employs in a convincing way.

In summary, the proposed framework consists of artefacts for subject-matter-specific inputs and an inner part that processes these inputs so that it can provide a compliant change management in CC-related scenarios. In the following chapters, the framework will be validated and evaluated following rigorous state-of-the-art scientific approaches.

[8] See Footnote 7 for details about these industry approaches

[9] See Footnote 5 for the complete text of the catalogue in German

5 Validation of the framework by experts

In this chapter, the external expert validation conducted is described. The overall aim of this validation is to gather feedback from different experts in the environment of the framework.

5.1 Validation Approach

To ensure the validity of the framework is necessary to have the opinion of several experts in the field. This will provide the opportunity to modify, adapt and improve the primordial design. Thus, there is a need on obtaining a collective understanding of subjective experts' views, an interpretive theoretical perspective was selected. This approach leads naturally to qualitative methodology, with methods that involve significant interaction with people directly experiencing the phenomena under investigation. Such qualitative approaches are not uncommon in information systems research e.g. (Goldkuhl, 2011; Marshall, Cardon, Poddar, & Fontenot, 2013; Sarker, Xiao, & Beaulieu, 2013; Venkatesh et al., 2013). Shanteau (1992) describes an expert as an individual who has been recognized within his or her profession as having the necessary skills and abilities to perform at the highest level. Because of their competence, expert groups are often used in consultation processes, because groups have more informational resources at their disposal than individuals do (Franz & Larson, 2002). In such settings, overlapping competence is useful, because it acts as a common ground among group members and facilitates learning (Kasvi, Vartiainen, Pulkkis, & Nieminen, 2000). As a consequence of its attractiveness, experts' judgements have been widely used in the information systems arena (Bergvall-Kåreborn & Howcroft, 2014; Chang, 2005; Mokhtar, Yusof, Ahmad, & Jambari, 2016; Paré, Cameron, Poba-Nzaou, & Templier, 2013; Saeed & Abdinnour, 2013; Worrell, Di Gangi, & Bush, 2013). The validation by experts designed for this thesis will be developed by means two different steps.

1. Validation of each of the items in the framework in an isolated way to ensure the validity of the tools (questionnaires) considered in each item of the framework and the validity of the suggested questions.
2. Validation of the framework as a whole by experts in the field.

In the following sections the two steps will be described in terms of design, data collection and analysis.

5.2 Validation of the items of the framework

The specifics of the framework items to be validated (legal, technological, processual/ organizational, cultural) required separate groups of experts in the corresponding areas. Therefore, validations were conducted in separate activities that are described for each area in the following. The descriptions include:

- The approach followed for the selection of experts, including the required or optional qualifications,
- The preparation of the workshops,
- The conduction of the workshops and their results, as well as the
- Follow-up activities after the workshop was conducted.

The sequence of the documentation of these validation workshops that follows, does not reflect the chronology of workshop conductions as some workshops were conducted in parallel.

With regards to the specific methodology adopted to perform the validation, it is based on experts' workshops. According to the Cambridge Dictionary a workshop is a meeting of people to discuss and/or perform practical work in a subject or activity. The aim is double: to refine the first input of the questionnaire and to validate the preliminary adopted.

5.2.1 Validation of Framework Items related to Legal Aspects

5.2.1.1 Selection of Experts

The validation of framework items related to legal aspects required the acquisition of experts with the following profile:

- University Education (ideally a master degree) in a related field (ideally law, management or IT management also possible);
- At least 5 years of experience in the relevant areas with at least 2 years of experience in a decision-making position;
- Working knowledge of Business English and Legal English (optional)

After an identification of 15 suitable experts they were contacted. 4 of them expressed interest and willingness to participate in the validation. This was a proper number for the conduction of the workshop as 3-5 participants were considered as ideal.

5.2.1.2 Workshop Preparation

The selected experts were provided with a detailed description of the proposed framework and with the complete relevant part of the framework at the current stage (in this case Subsection 4.4). Furthermore, they were provided with the specific questions they were expected to answer at the workshop:

- Is the given framework a sufficient tool to define risks?
- Are there other areas for influences or risks for cloud computing/cloud services?
- If yes, which are these other areas?
- What is the importance of each of the presented areas from the point of view of the experts?
- Are questionnaires helpful in finding inputs in the specific subject field (e.g., legal) for the purpose of risk assessment of the framework?
- Are there any questions that are unclearly formulated or other clarifications necessary?
- Are there any questions that are not necessary or redundant and should therefore be removed from the questionnaire?
- Are there any relevant questions that have not been considered until now and should therefore be added to the questionnaire?
- Further remarks or recommendations.

5.2.1.3 Workshop Conduction and Results

The assessment workshop LEGAL was conducted in the third quarter of 2015 in Berlin, Germany. Workshop participants were provided with an ample meeting room with all necessary facilities (beamer, smartboards and flipcharts).

The experts spent the day addressing the specific questions that they have received in advance (see previous section). More specifically, the following types of results were planned:

- A consensus decision (yes/no) regarding the first question (Is the given framework a sufficient tool to define risks?),
- A consensus decision (yes/no) regarding the second question (Are there other areas for influences or risks for cloud computing/cloud services?),
- An (optional) list regarding the third question (If yes, which are these other areas?),
- A consensus decision regarding the fourth question (What is the importance of each of the presented areas from the point of view of the experts?)
- A consensus decision (yes/no) regarding the fifth question (Are questionnaires helpful in finding inputs in the specific subject field (e.g., legal) for the purpose of risk assessment of the framework?),
- An agreed upon list of existing questions in the questionnaire that need to be improved (as answer to the sixth question – Are there any questions that are unclearly formulated?),
- An agreed upon list of existing questions in the questionnaire that need to be removed (as answer to the third question – Are there any questions that

are not necessary or redundant and should therefore be removed from the questionnaire?), and
- A list with further recommendations from the experts.

The workshop was moderated by the author and it provided the following validation results.

General Appropriateness of the Proposed Tool

The proposed tool was considered appropriate to assess the subject area. More specifically, experts answered the first question with "yes", the second with "no" (resulting in an empty list as answer to the third question).

The legal environment was considered as the most important area from the experts.

Proposed Clarifications

- Several clarifications were suggested (see Figure 11):
  - A clear definition of "change" needs to be provided,
  - The notion of "risk" should be described more precisely,
  - The triggers for changes in the subject area (e.g., personal, political, economic) should be considered in more details.
  - Importance and frequency of triggers should be considered (see Figure 12 and Figure 13).

Questions that should be removed

The summary assessment for all questions is shown in Figure 14. Questions that should be removed are shown in the middle column. The experts recommend the removal of the following questions:

- Question # 5,
- Question # 7,
- Question # 14, and
- Question # 15, while
- Question # 17 should be reformulated.

Questions that should be added

Questions that should be added are shown in the right column of Figure 14. The experts recommend the addition of the following questions:

- Is international data communication affected by the change?
- Are sanctions anticipated?
- Are there access points for state agencies (e.g. NSA)
- Are there any explicit restrictions?

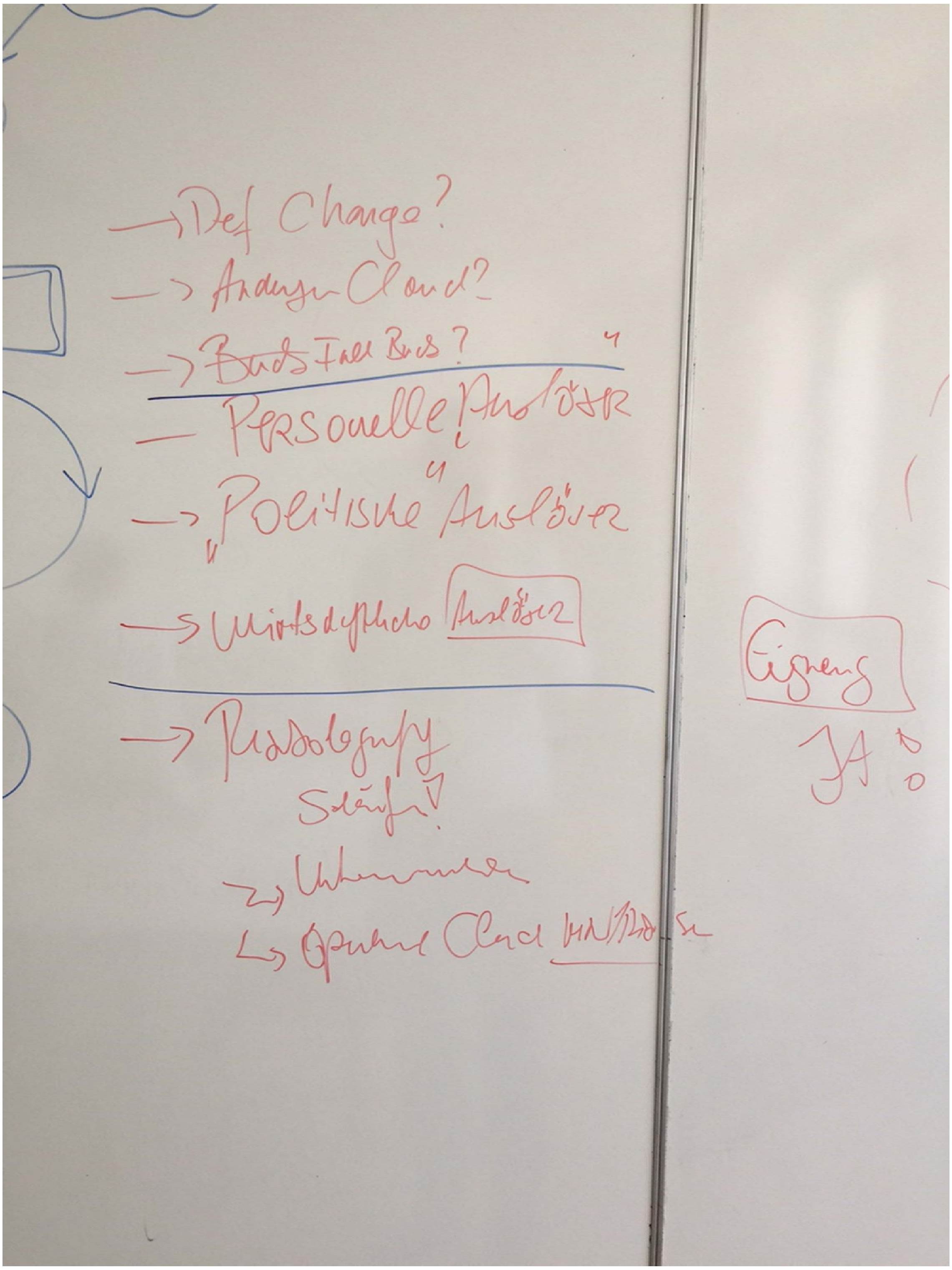
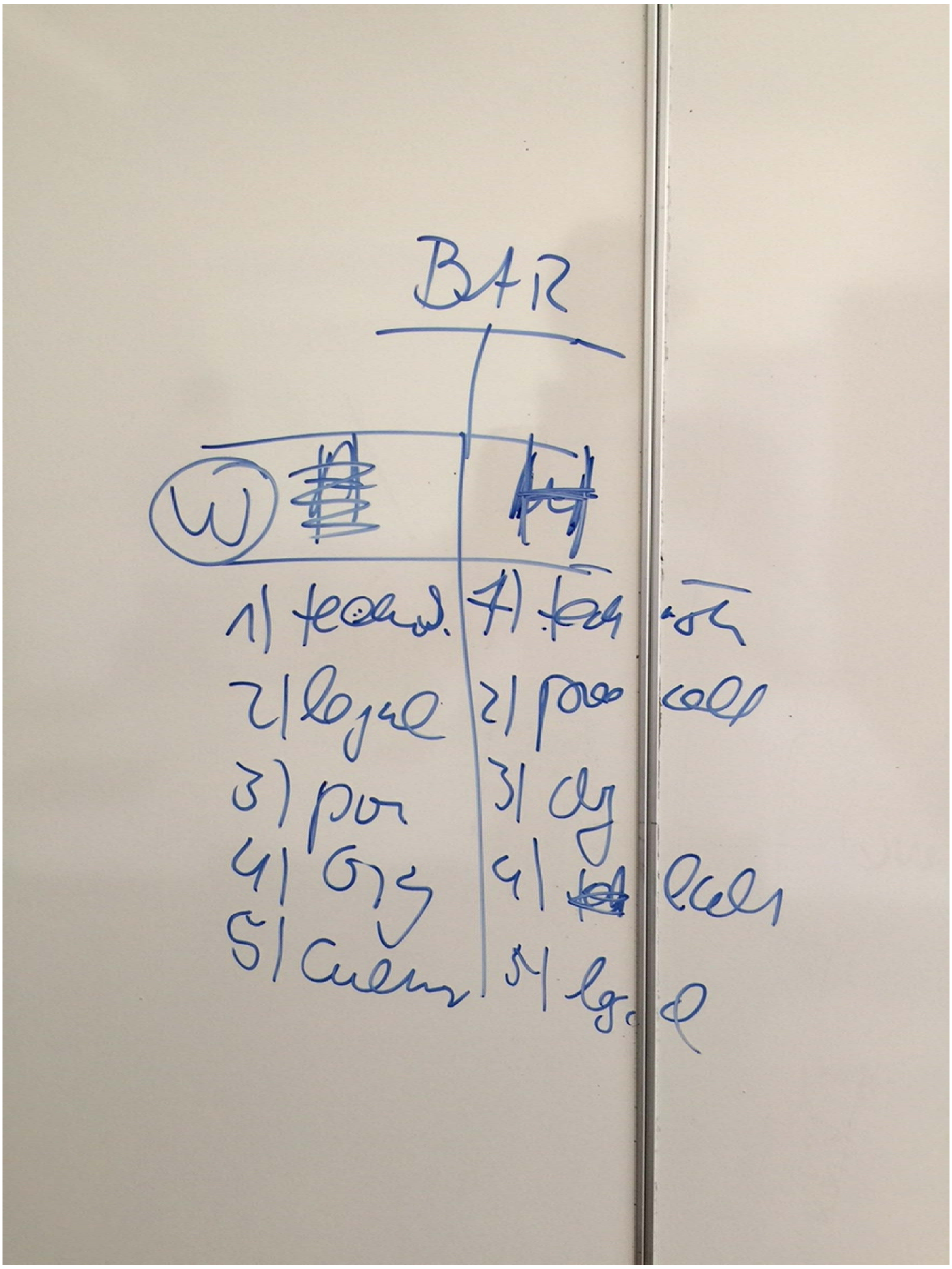


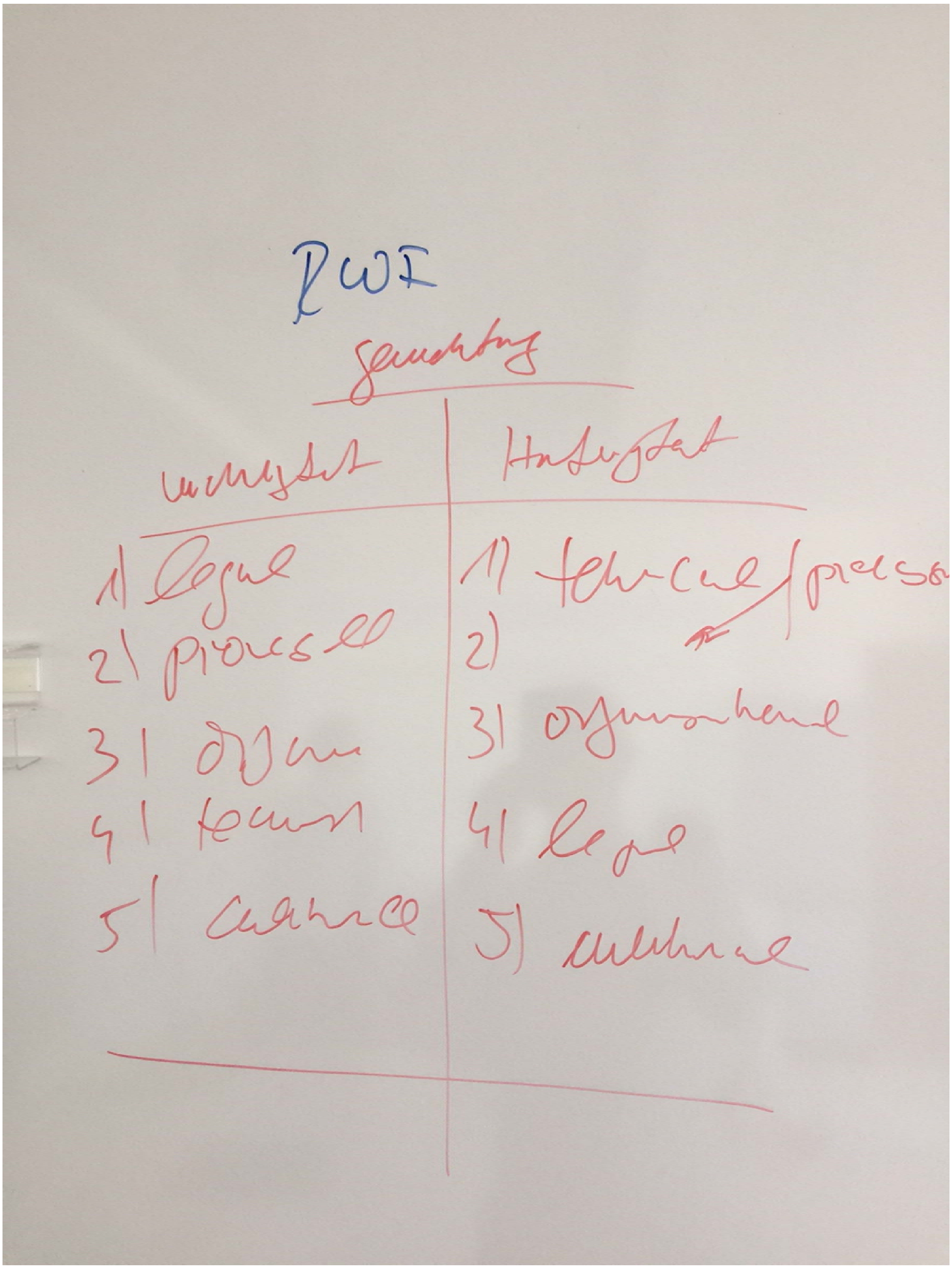
Figure 11. Documentation of Suggested Clarification in LEGAL area (in German)



BAR

W	H
1) techn.	1) techn [illegible]
2) legal	2) proc coll
3) proc	3) org
4) org	4) ~~[illegible]~~ local
5) cultur	5) legal

Figure 12. Documentation of Suggested Frequency (W) and Frequency (H) of Triggers from Expert 1



RWI

Gewichtung

Wichtigkeit	Häufigkeit
1) legal	1) technical / process
2) prozesse	2)
3) organ	3) organizational
4) techn	4) legal
5) cultural	5) cultural

Figure 13. Documentation of Suggested Frequency (left) and Frequency (right) of Triggers from Expert 2

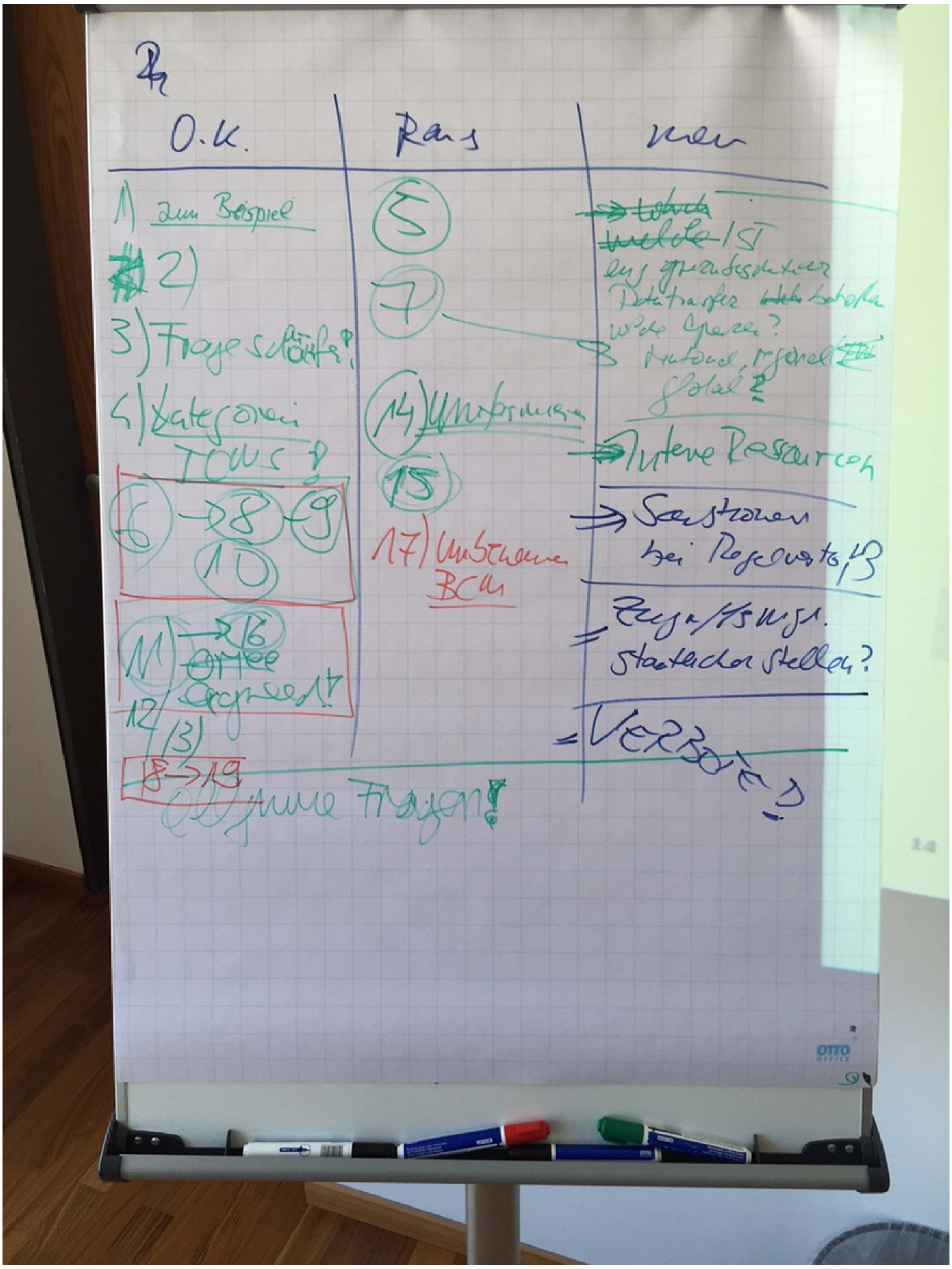


Figure 14. Summary of Assessment all Questions – left column (ok), middle column (to be removed), right column (to be added)

5.2.1.4 Follow-Up Activities

The follow-up activities in the aftermath of the workshop were as follows:

- Validation and clarification of results,
- Implementation of improvement into the specific area of the framework (see following Chapter 6), and
- Consideration of possible effects to other areas of the framework.

5.2.2 Validation of Framework Items related to Organizational and Processual Aspects

5.2.2.1 Selection of Experts

The validation of framework items related to organizational and processual aspects required the acquisition of experts with the following profile:

- University Education (ideally a master degree) in a related field (ideally management or IT management, other related fields also possible);
- At least 5 years of experience in the relevant areas with at least 2 years of experience in a decision-making position;
- Working knowledge of Business English and Legal English (optional)

After an identification of 15 suitable experts they were contacted. 3 of them expressed interest and willingness to participate in the validation. This was a proper number for the conduction of the workshop as 3-5 participants were considered as ideal.

5.2.2.2 Workshop Preparation

The selected experts were provided with a detailed description of the proposed framework and with the complete relevant part of the framework at the current stage (in this case Subsection 4.5). Furthermore, they were provided with the specific questions they were expected to answer at the workshop:

- Is the given framework a sufficient tool to define risks?
- Are there other areas for influences or risks for cloud computing/cloud services?
- If yes, which are these other areas?
- What is the importance of each of the presented areas from the point of view of the experts?
- Are questionnaires helpful in finding inputs in the specific subject field (e.g., organizational) for the purpose of risk assessment of the framework?
- Are there any questions that are unclearly formulated or other clarifications necessary?

- Are there any questions that are not necessary or redundant and should therefore be removed from the questionnaire?
- Are there any relevant questions that have not been considered until now and should therefore be added to the questionnaire?
- Further remarks or recommendations.

5.2.2.3 Workshop Conduction and Results

The assessment workshop ORGANIZATIONAL and PROCESSUAL was conducted in the third quarter of 2015 in Berlin, Germany. Workshop participants were provided with an ample meeting room with all necessary facilities (beamer, smartboards and flipcharts).

The experts spent the day addressing the specific questions that they have received in advance (see previous section). More specifically, the following types of results were planned:

- A consensus decision (yes/no) regarding the first question (Is the given framework a sufficient tool to define risks?),
- A consensus decision (yes/no) regarding the second question (Are there other areas for influences or risks for cloud computing/cloud services?),
- An (optional) list regarding the third question (If yes, which are these other areas?),
- A consensus decision regarding the fourth question (What is the importance of each of the presented areas from the point of view of the experts?)
- A consensus decision (yes/no) regarding the fifth question (Are questionnaires helpful in finding inputs in the specific subject field (e.g., organizational) for the purpose of risk assessment of the framework?),
- An agreed upon list of existing questions in the questionnaire that need to be improved (as answer to the sixth question – Are there any questions that are unclearly formulated?),
- An agreed upon list of existing questions in the questionnaire that need to be removed (as answer to the third question – Are there any questions that are not necessary or redundant and should therefore be removed from the questionnaire?), and
- A list with further recommendations from the experts.

General Appropriateness of the Proposed Tool

The proposed tool was considered appropriate to assess the subject area. More specifically, experts answered the first question with "yes", the second with "no" (resulting in an empty list as answer to the third question).

The organizational and processual environment was considered as the most important area from the experts.

Proposed Clarifications

- Several clarifications were suggested:
    - A categorization of processes in the levels of "governance processes", "customer-facing processes", "core processes", and "support processes" should be considered;
    - Questions should be considered that allow a quantitative assessment of risks and their significance, e.g., questions with Likert scale;
    - Questions that concern existing processes should consider differentiation in categories, e.g. "must do", "nice-to-have", "delighter".

Questions that should be removed

Questions that should be removed were not named by the experts.

Questions that should be added

Questions that should be added were also suggested. The experts recommend the addition of the following questions:

- Are business impact analyses being conducted?
- Are there specific defined strategies and related KPIs for them at the process level?

5.2.3 Validation of Framework Items related to Technological Aspects

5.2.3.1 Selection of Experts

The validation of framework items related to technological aspects required the acquisition of experts with the following profile:

- University Education (ideally a master degree) in Computer science, Information Systems or related field (ideally management or IT management, other related fields also possible);
- At least 5 years of experience in the relevant areas with at least 2 years of experience in a decision-making position;
- Working knowledge of Business English and Legal English (optional)

After an identification of 15 suitable experts they were contacted. 5 of them expressed interest and willingness to participate in the validation. Again, this was a proper number for the conduction of the workshop.

5.2.3.2 Workshop Preparation

The selected experts were provided with a detailed description of the proposed framework and with the complete relevant part of the framework at the current stage by that time. Furthermore, they were provided with the specific questions they were expected to answer at the workshop:

- Is the given framework a sufficient tool to define risks?
- Are there other areas for influences or risks for cloud computing/cloud services?
- If yes, which are these other areas?
- What is the importance of each of the presented areas from the point of view of the experts?
- Are questionnaires helpful in finding inputs in the specific subject field (e.g., technological) for the purpose of risk assessment of the framework?
- Are there any questions that are unclearly formulated or other clarifications necessary?
- Are there any questions that are not necessary or redundant and should therefore be removed from the questionnaire?
- Are there any relevant questions that have not been considered until now and should therefore be added to the questionnaire?
- Further remarks or recommendations.

5.2.3.3 Workshop Conduction and Results

The assessment workshop TECHNOLOGICAL was conducted in the third quarter of 2015 in Berlin, Germany. Workshop participants were provided with an ample meeting room with all necessary facilities (beamer, smartboards and flipcharts).

The experts spent the day addressing the specific questions that they have received in advance including the ones presented in the list in the previous question. More specifically, the following types of results were planned:

- A consensus decision (yes/no) regarding the first question (Is the given framework a sufficient tool to define risks?),
- A consensus decision (yes/no) regarding the second question (Are there other areas for influences or risks for cloud computing/cloud services?),
- An (optional) list regarding the third question (If yes, which are these other areas?),
- A consensus decision regarding the fourth question (What is the importance of each of the presented areas from the point of view of the experts?)
- A consensus decision (yes/no) regarding the fifth question (Are questionnaires helpful in finding inputs in the specific subject field (e.g., technical) for the purpose of risk assessment of the framework?),

- An agreed upon list of existing questions in the questionnaire that need to be improved (as answer to the sixth question – Are there any questions that are unclearly formulated?),
- An agreed upon list of existing questions in the questionnaire that need to be removed (as answer to the third question – Are there any questions that are not necessary or redundant and should therefore be removed from the questionnaire?), and
- A list with further recommendations from the experts.

General Appropriateness of the Proposed Tool

The proposed tool was considered appropriate to assess the subject area. More specifically, experts answered the first question with "yes", the second with "yes", and provided no further input as an answer to the third question.

The technological environment was considered to be the most dynamic area from the experts. They expect that assessments of this environment will be conducted more often that assessments in some of the other fields.

Proposed Clarifications

- Several clarifications were suggested:
  - A clearer structure and better wording of Questions 10;
  - A clearer structure and better wording of Questions 11;
  - A clearer structure and better wording of Questions 12;
  - A clearer structure and better wording of Questions 13;
  - A clearer structure and better wording of Questions 14;
  - A clearer structure and better wording of Questions 15;

Questions that should be removed

Questions that should be removed were not named by the experts.

Questions that should be added

Questions that should be added were not suggested.

5.2.4 Validation of Framework Items related to Cultural Aspects

5.2.4.1 Selection of Experts

The validation of framework items related to organizational and processual aspects required the acquisition of experts with the following profile:

- University Education (ideally a master degree) in a related field (ideally management or IT management, other related fields also possible);

- At least 5 years of experience in the relevant areas with at least 2 years of experience in a decision-making position;
- Working knowledge of Business English and Legal English (optional)

After an identification of 15 suitable experts they were contacted. 3 of them expressed interest and willingness to participate in the validation. This was a proper number for the conduction of the workshop as 3-5 participants were considered as ideal.

5.2.4.2 *Workshop Preparation*

The selected experts were provided with a detailed description of the proposed framework and with the complete relevant part of the framework at the current stage (in this case Subsection 4.7). Furthermore, they were provided with the specific questions they were expected to answer at the workshop:

- Is the given framework a sufficient tool to define risks?
- Are there other areas for influences or risks for cloud computing/cloud services?
- If yes, which are these other areas?
- What is the importance of each of the presented areas from the point of view of the experts?
- Are questionnaires helpful in finding inputs in the specific subject field (e.g., cultural) for the purpose of risk assessment of the framework?
- Are there any questions that are unclearly formulated or other clarifications necessary?
- Are there any questions that are not necessary or redundant and should therefore be removed from the questionnaire?
- Are there any relevant questions that have not been considered until now and should therefore be added to the questionnaire?
- Further remarks or recommendations.

5.2.4.3 *Workshop Conduction and Results*

The assessment workshop CULTURAL was conducted in the third quarter of 2015 in Madrid, Spain. Workshop participants were provided with an ample meeting room with all necessary facilities (beamer, smartboards and flipcharts).

The experts spent the day addressing the specific questions that they have received in advance (see previous section). More specifically, the following types of results were planned:

- A consensus decision (yes/no) regarding the first question (Is the given framework a sufficient tool to define risks?),

- A consensus decision (yes/no) regarding the second question (Are there other areas for influences or risks for cloud computing/cloud services?),
- An (optional) list regarding the third question (If yes, which are these other areas?),
- A consensus decision regarding the fourth question (What is the importance of each of the presented areas from the point of view of the experts?)
- A consensus decision (yes/no) regarding the fifth question (Are questionnaires helpful in finding inputs in the specific subject field (e.g., cultural) for the purpose of risk assessment of the framework?),
- An agreed upon list of existing questions in the questionnaire that need to be improved (as answer to the sixth question – Are there any questions that are unclearly formulated?),
- An agreed upon list of existing questions in the questionnaire that need to be removed (as answer to the third question – Are there any questions that are not necessary or redundant and should therefore be removed from the questionnaire?), and
- A list with further recommendations from the experts.

General Appropriateness of the Proposed Tool

The proposed tool was considered appropriate to assess the subject area. More specifically, experts answered the first question with “yes”, the second with “yes”, and provided the following list as an answer to the third question:

- Military, and
- Politics.

The cultural environment was considered to be the most important area from the experts. More specifically, three of Hofstede´s cultural dimensions – Uncertainty Avoidance Index (UAI); Long Term Orientation versus Short Term Normative Orientation (LTO) and Power Distance (PDI) were named as “really crucial measures for almost any development in the world.”

Proposed Clarifications

- Several clarifications were suggested:
  - A more clear focus on the framework objectives,
  - Consideration of aspects of national culture, and
  - Consideration of aspects of organizational culture.

Questions that should be removed

Questions that should be removed were not named by the experts.

Questions that should be added

Questions that should be added were also suggested. The experts recommend the addition of the following questions:

- What aspects of national culture do you consider relevant?
- What aspects of organizational culture do you consider relevant?

5.2.5 Summary of Framework Items Validation

In general, the validation provided the intended benefits for the framework. Beside the validation and improvement of items in the different subject areas, it provided a necessary and useful multi-disciplinary view at the framework. The specific worldviews of the experts in the different areas can be summarized as follows:

1. The experts from the legal area focused on the need of proper definitions, e.g. the definition of "change".
2. The experts from the processual and organizational area focused on the need of clear process categories from organizational point of view (e.g. "governance processes", "core processes", "support processes") and from the point of view of their necessity ("must-do", "nice-to-have", "delighter"). Furthermore, they emphasized the importance of KPIs related to specific strategies and suggested a more quantification-oriented approach of the questionnaire.
3. The experts from the technological area stressed the importance of technological trends and developments and of specific deployment and implementation approaches.
4. The experts from the cultural area identified further possible areas of influence (military, politics) and stressed the importance of specific cultural dimensions, e.g. Uncertainty Avoidance Index (UAI), Long Term Orientation versus Short Term Normative Orientation (LTO), Power Distance (PDI)…

The consideration of validation results and how they are reflected in the framework is the subject of the next chapter.

5.3 Validation of the framework as a whole

In the case of the validation of the framework as a whole, the vehicle for obtaining the views of the experts is the "Expert Assessment Questionnaire", whose design reflects the following structure:

- Framework objectives
  - Do you consider adequate the aim of the framework?
- Methodology
  - What is your opinion on the methodology used for the design of the framework?

- Theoretical innovation
  - Is there any theoretical contribution in the framework?
- Applicability
  - What is the applicability of the framework?
- Suggestions for improvement
  - What aspects of the framework designed (questionnaires, implementation ...) could be improved?

The questionnaire is designed to be sent to appointed experts by email. Experts will fill the questionnaire in a remote way assisted by Ph.D. candidate. This questionnaire was proved in different settings (Colomo-Palacios, Casado-Lumbreras, Soto-Acosta, García-Peñalvo, & Tovar-Caro, 2013; Colomo-Palacios, Tovar-Caro, García-Crespo, & Gómez-Berbís, 2010; Ruano-Mayoral, Colomo-Palacios, Fernández-González, & García-Crespo, 2011) and was adapted to the specific aims of the framework. The questionnaire consists of open questions that inquire about various aspects: methodological rigor, theoretical innovation, practical utility, etc. Such open-ended questionnaires are, again, pervasive in information systems research (Baskerville & Myers, 2015; Kaplan & Duchon, 1988; Mingers, 2003; Silverman, 1998).

5.3.1 Data collection

The process of data collection consisted in the identification and selection of the experts involved in the validation. Therefore, in this subsection, the selection criteria used for expert groups is explained. Careful expert selection for these studies is needed to avoid threats of validity. In order to prevent bias, uncertainty and incompleteness to the maximum extent possible, a careful expert selection must be adopted (Freimut, Briand, & Vollei, 2005).

Experts were drawn from both academia and industry, using a range of techniques. Some potential interviewees from industry were identified based on prior working relationship with them and other networking activities. Potential candidates from academia were identified through personal contacts. To participate in this study, fifteen experts in the field were invited by e-mail to participate but just six agreed to participate. Participants were fully informed about the implications of their involvement in the research and to comply with ethical issues, each expert was provided with a research profile.

5.3.2 Analysis

Considering the analysis of the questionnaires received, we can draw the following conclusions:

- Framework objectives: All selected experts have positively assessed the main objective of this thesis: the design of a framework for compliance management in CC environments driven by change management. The experts understand that due to the generalization of CC and the increasing pressure on compliance management, research to promote knowledge and practice of compliance is necessary.
- Methodology: Experts have agreed that the design and use of qualitative methodological approaches and literature reviews guarantee the construction of an adequate framework.
- Theoretical innovation: So far, there is little literature aimed at improving the effectiveness of the compliance process in CC settings. The results obtained in the implementation of the framework will represent an advance in the knowledge of the management of compliance matters. In this regard, experts predict that the implementation of the framework will confirm the relevance of the process and, at the same time, confirm the need for frameworks to guide the management of these processes.
- Applicability: The results obtained after the implementation of the framework will be potentially applicable to other projects and can even generate the need to create frameworks to guide other key processes in CC settings.
- Suggestions for improvement: With regards to the areas for improvement or modification, the following aspects are considered noteworthy:
    - One expert notes the time consumed in the questionnaires and the need to count on specific support for the implementation of the framework. He suggest that, in order to increase the impact of a possible future commercialization, a more automated support will be needed.
    - Another expert is concerned with the maintainability of the aspects of the framework. This subject believes that some of the aspects of the framework will suffer volatility and obsolescence.
    - Several aspects were reported by experts that leaded to the enhancement of the questionnaires in terms of expressions to improve readability. As a result of this process, several items where rewritten based on the experts' opinions.

6 Adaptation of the Framework after Validation

The validation of the framework provided – beside the general confirmation of its appropriateness and feasibility – also a range of improvement suggestions regarding both the number of questions included in a specific questionnaire and the specific wording of questions.

In the following, the consideration of these validation results is described for the specific areas of the framework. Furthermore, the new version of the framework items that implement the suggested improvement is presented.

6.1 Legal Area

6.1.1 Consideration of Improvement Suggestions

In the legal area, several clarifications were suggested:

- A clear definition of "change" needs to be provided,
- The notion of "risk" should be described more precisely,
- The triggers for changes in the subject area (e.g., personal, political, economic) should be considered in more details.
- Importance and frequency of triggers should be considered.

These clarifications are important and are considered in the subsequent adaptation of the framework in the legal area.

The experts recommend the removal of the following questions:

- Question # 5,
- Question # 7,
- Question # 14, and
- Question # 15, while
- Question # 17 should be reformulated.

This recommendation is considered helpful and is reflected in the subsequent adaptation of the framework in the legal area.

The experts recommend the addition of the following questions:

- Is international data communication affected by the change?
- Are sanctions anticipated?
- Are there access points for state agencies (e.g. NSA, BND)
- Are there any explicit restrictions?

This recommendation is considered helpful and is reflected in the subsequent adaptation of the framework in the legal area.

6.1.2 Framework Adaptation

This questionnaire is the improved version of the questionnaire presented in Section 4.4 and includes changes reflecting the suggestions from the experts during the validation phase.

Preliminary questions/inquiries:

Please, provide your organizational definitions of "change" and "risk"!

Table 13. Improved Version of Questionnaire for Legal Environment after Validation

#	Question
1.	Which data is affected by the outsourcing decision? Higher risk data such health-related, social, or medically confidential?
2.	Which legal frameworks are applicable?
3.	Which existing risks are associated with the outsourcing decision: data availability, confidentiality, or integrity?
4.	Which requirements exist concerning data protection: appropriate security architecture, data encryption and cryptography, identity and rights management, control possibilities, monitoring and security incident management, contingency plans and measures, and others?
5.	Is the provider compliant with legal and data protection requirements?
6.	Does the provider have an information security management system (ISMS) concept?
7.	How was the ISMS concept assessed concerning appropriateness of technical and organizational measures and how is the result of the assessment documented?
8.	Does the provider have current and internationally established certifications (for example, ISO 27001)?
9.	Is the cloud computing service precisely and clearly formulated?
10.	Are appropriate control rights for the cloud user organization and corresponding obligations for the cloud provider being specified?
11.	Are there clauses that govern the contingency operation and the return of data in the case of bankruptcy of the cloud provider?

12.	Are there specific, relevant service-level agreements? Do they outline the availability and dependability requirements, response and restoration deadlines, computing power, and support details?
13.	Are there specific Business Continuity Management (BCM) regulations for the case of catastrophic failures?
14.	Are controls being conducted regularly? Are there assessments of the agreed-upon technical and organizational measures?
15.	Are the security concepts being regularly assessed? Are they current, and do they correspond to the current state of the art?
16.	Is international data communication affected by the change?
17.	Are sanctions anticipated?
18.	Are there access points for state agencies (e.g. NSA)
19.	Are there any explicit restrictions?

This new and improved version of the questionnaire will be used in the evaluation of the framework.

6.2 Organizational and Processual Area

6.2.1 Consideration of Improvement Suggestions

In the organizational and processual area, several clarifications were suggested:

- A categorization of processes in the levels of “governance processes”, ”customer-facing processes”, “core processes”, and “support processes” should be considered;
- Questions should be considered that allow a quantitative assessment of risks and their significance, e.g., questions with Likert scale;
- Questions that concern existing processes should consider differentiation in categories, e.g. “must do”, “nice-to-have”, “delighter”.

These clarifications are important. Most of them are considered in the subsequent adaptation of the framework in the organizational and processual area.

The experts recommend the removal of the following questions:

- none.

This recommendation is considered helpful and is reflected in the subsequent adaptation of the framework in the organizational and processual area.

The experts recommend the addition of the following questions:

- Are business impact analyses being conducted?
- Are there specific defined strategies and related KPIs for them at the process level?

This recommendation is considered helpful and is reflected in the subsequent adaptation of the framework in the organizational and processual area.

6.2.2 Framework Adaptation

This questionnaire is the improved version of the questionnaire presented in Section 4.5 and includes changes reflecting the suggestions from the experts during the validation phase.

Table 14. Improved Version of Questionnaire for Organizational and Processual Environment after Validation

#	Question
1.	Are there existing guidelines for the introduction of changes in processes and in process steps? What are the effects of such changes on other processes? What are the effects of such changes on the corporate strategy? Is it assured that security aspects are to be considered during the introduction of changes? Are all changes planned, tested, approved and documented? Are fallback solutions developed before the implementation of changes? Is the information security management involved in all substantial changes?
2.	Are enterprise-critical processes affected? How about the data availability in these processes? Effects on the availability of other processes?
3.	Are there changes in the responsibilities and roles resulting from the change?
4.	Emergency Plan Assessment of the documentation of latest emergency tests Security concept Routine security assessments at the CSP and other contractors by certified third party Authentication, authorization, administration, audits, awareness access control Data processing is allowed solely according to the instructions of the cloud user, no data usage by the CSP for own purposes Penetration tests at the CSP and other contractors Monitoring by the cloud user should be possible, SLA fulfilment should be provable Logging and monitoring of administrator activities Four-eyes-principle during critical administration activities Provision of log files by the CSP Information about security incidents 24/7 response team for Security Incident Handling and Trouble Shooting 24/7 Monitoring of cloud services and an immediate response to security incidents Implementation of proper measures against internal threats that are inherent in a multi-tenant architecture

	Establishment of transparency and trust by the provision of detailed information intended for the cloud user Measures at the personnel level Police certificate Educational history, qualifications, current and past affiliations Personal environment (e.g. party membership) Courses in IT security Courses in social engineering Control and education for awareness Assessment of contractors (e.g., technicians, facility managers) Data security and non-disclosure agreements
5.	What types of processes are affected? • Depending on their areas, e.g. "governance processes", "customer-facing processes", "core processes", and "support processes"; • Depending on their necessity and importance, e.g. "must do", "nice-to-have", "delighter".
6.	Are business impact analyses being conducted?
7.	Are there specific defined strategies and related KPIs for them at the process level?

This new and improved version of the questionnaire will be used in the evaluation of the framework.

6.3 Technological Area

6.3.1 Consideration of Improvement Suggestions

In the technological area, several clarifications were suggested:

- A clearer structure and better wording of Questions 10;
- A clearer structure and better wording of Questions 11;
- A clearer structure and better wording of Questions 12;
- A clearer structure and better wording of Questions 13;
- A clearer structure and better wording of Questions 14;
- A clearer structure and better wording of Questions 15;

These clarifications are important. Most of them are considered in the subsequent adaptation of the framework in the organizational and processual area.

The experts recommend the removal of the following questions:

- none.

This recommendation is considered helpful and is reflected in the subsequent adaptation of the framework in the technological area.

The experts recommend the addition of the following questions:

- none.

This recommendation is considered helpful and is reflected in the subsequent adaptation of the framework in the technological area.

6.3.2 Framework Adaptation

Table 15. Improved Version of Questionnaire for Technological Environment after Validation

#	Question
1.	What technologies are available for user and access management, role-based access control, two factor authentication?
2.	What technologies are available for encryption during data processing and data transport?
3.	What technologies are available for data backup, restoration and availability of the service?
4.	What technologies are available for redundant supply of power, HVAC, water?
5.	What technologies are available for fire protection?
6.	What technologies are available for robust infrastructure, redundant network connection, emergency working places etc?
7.	What technologies are available for redundant data centres, documentation and control of availability management?
8.	What technologies are available for building security, access control, and secure entry area?
9.	What technologies are available for control of service contractors (cleaning, facility management, repair technicians)?
10.	What technologies are available for assuring server security? - Host protection (firewall, intrusion detection, integrity checking) - Secure standard configuration (beefed-up operating system) - Sandboxed environment for every virtual machine - Certified hypervisors (at least CC EAL4, IT SEC E3) - Redundant images / services of the provided - A secure sandbox environment in the case of IaaS in order to prevent exploits on host systems - Systems in place for assessment of system documentation, status, log files
11.	What technologies are available for assuring network security? - Redundant network links - Safeguards against attacks, malware and viruses - Secure configuration of all cloud components, network segmentation - Encrypted remote administration - Encrypted communication between CSP and cloud user - Encrypted communication between different CC sites

	- Encrypted communication to and from third-party contractors - Encrypted transmission of network management information - Analysis of VPN infrastructure and end-to-end encryption chain
12.	What technologies are available for assuring application and platform security? - Integration of security management into the software life cycle, security gates, vulnerability tests, audits, code reviews etc. - Application isolation, interface monitoring - Automatic monitoring and assessment of user applications - Patch and change management, patch compatibility tests - Control whether guidelines for development of secure applications are applied
13.	What technologies are available for assuring information security? - Patch and change management - Definition of life cycle of customer data - Secure isolation - Role-based information access, e.g. based on LDAP - Regular backups (extent, intervals, storage concept, times and durations) - Complete and secure deletion - Every component can be targeted by an attack; therefore, analysis of weaknesses and protection measures is needed (end-to-end security)
14.	What technologies are available for assuring encryption and key management? - Only assured and secure encryption methods are used - Random generated keys with sufficient key length - Secure asynchronous key exchange - Short duration of keys, secure storage of keys - Key destruction, e.g. utilizing SAML - Strong authentication of cloud users (two-factor authentication)
15.	What technologies are available for overcoming the lack of standardization in CC? - The customer should ensure if the provider uses standardized technology and interfaces; this should be mentioned in its initial contract. - Hybrid cloud approaches to avoid compatibility issues between cloud and IT systems in customer's organization

This new and improved version of the questionnaire will be used in the evaluation of the framework.

6.4 Cultural Area

6.4.1 Consideration of Improvement Suggestions

In the cultural area, several clarifications were suggested:

- A clearer focus on the framework objectives,
- Consideration of aspects of national culture, and

- Consideration of aspects of organizational culture.

These clarifications are important. Most of them are considered in the subsequent adaptation of the framework in the cultural area.

The experts recommend the removal of the following questions:

- none.

This recommendation is considered helpful and is reflected in the subsequent adaptation of the framework in the cultural area.

The experts recommend the addition of the following questions:

- What aspects of national culture do you consider relevant?
- What aspects of organizational culture do you consider relevant?

This recommendation is considered helpful and is reflected in the subsequent adaptation of the framework in the cultural area.

6.4.2 Framework Adaptation

This questionnaire is the improved version of the questionnaire presented in Section 4.7 and includes changes reflecting the suggestions from the experts during the validation phase.

Table 16. Improved Version of Questionnaire for Cultural Environment after Validation

#	Question
1.	What are the countries of incorporation of headquarters, main offices and branches of the organization?
2.	What are the countries of incorporation of main accounts of the organization?
3.	What market reach does the organization have (regional, national, international and world-wide?
4.	What other predominant cultural aspects exist (e.g. a religious or non-profit organization, military or other specific organizational environments)?
5.	What are the relevant cultural dimensions (according to Hofstede and subsequent works) for the organization?
6.	Which metrics about the relevant cultural dimensions are needed?
7.	How are needed metrics about the relevant cultural dimensions accumulated?
8.	What is the relevance of every relevant cultural dimension for the change management?
9.	How are the relevant metrics considered during the change process?
10.	What aspects of national culture do you consider relevant?

11.	What aspects of organizational culture do you consider relevant?

This new and improved version of the questionnaire will be used in the evaluation of the framework.

6.5 Summary of Framework Adaptation

The adaptation of the framework considered most of the improvements suggested by the experts during the validation phase. More specifically, questions were edited, removed and added in the areas of legal, organizational and processual, technological, and cultural aspects. Furthermore, cross-references (e.g., definitions "change" and "risk", objectives of the framework in cultural area) were introduced to improve the comprehensiveness of the framework. The so enhanced version of the framework is subjected to the evaluation that is described in the following chapter.

7 Evaluation

The aim of the evaluation is to verify that the framework proposed in this Ph.D. thesis improves compliance management in CC settings. This is done while taking into account research objectives, research questions and hypothesis presented in Chapter 1. The evaluation of the proposed thesis considers the evaluation approaches proposed for each section of the framework as well as an overall evaluation of the framework that will be generalized based on these area-specific evaluations. In this section, we detail the research methodology for the case studies conducted and continue with the data analysis and discussion of results.

7.1 Evaluation Approach

Evaluation consists of three different phases:

- Phase 1: Collecting information on compliance management in CC environments without the use of the framework. The purpose of this phase is the analysis of two different case studies with regard to compliance management but also with regard to other IT issues. During the daily activities of the two organizations, data shall be collected in order to obtain the information necessary to analyze their efforts.
- Phase 2: Collecting information on compliance management in CC environments using the framework defined in this Ph.D. thesis. The objective of this phase is to validate that it is possible to improve the compliance management by using the framework proposed in this thesis. The implementation of the framework in a real environment will reveal what aspects improve the situation that has been analyzed in Phase 1. The implementation of the framework will involve monitoring the project, as well as data collection for supporting the analysis of likeliness.
- Phase 3: Comparison between Phase 1 and Phase 2. In this phase, the goal is to compare compliance management with and without using the proposed framework, verifying or rejecting the hypotheses.

As already specified, the objective of this thesis is the definition of a compliance framework for outsourcing projects and the operating phase in a cloud service environment. The success criteria will therefore depend on reaching the following goals:

1. How to properly estimate the scope of the different input areas - legal, cultural, organizational, processual, and technical.
2. How to assess and classify the input from these areas in order to ensure consistency and prevent contradiction in change inputs.
3. How to properly formalize and plausibly assess the CC alternatives that may be suitable for every change request.
4. How to properly formalize and plausibly assess the compliance requirements of every change request.
5. How to properly formalize compliance capabilities of the CC alternatives.
6. How to properly compare and match compliance requirements and compliance capabilities.
7. How to properly represent both compliance requirements and compliance capabilities during the different phases of the change management cycle – request, categorization, risk assessment, and realization.
8. How to assess the impact of single changes to existing compliance requirements and the relevant controls addressing these requirements for the organization.
9. How to assess the impact of cumulative changes to existing compliance requirements and the relevant controls addressing these requirements for the organization.
10. How to map the benefits of the framework to specific agreed-upon KPIs.

The basic idea behind this evaluation is to compare the performance of change management in a cloud service environment before and after introducing the designed framework. This means, that specific KPIs of the organizations will initially be measured and documented before introducing the framework. Then, the framework will be implemented to a degree that is feasible and that reflects the specifics of the organization. A certain period of operation of the framework is needed after the implementation, before the effects of the framework can be observed. After this period is passed, a second measurement of the organization will be conducted. Finally, results of both measurements will be compared in order to estimate the meeting of the already defined success criteria. These three phases will be explained in the next section.

The organizations where this evaluation takes place should meet certain previously defined criteria. They should have a certain maturity of their IT operations, so that the topics of change management, compliance and cloud services have the proper relevance for the organization. Preferably these organizations should be privately owned and operating on the open market in order to reflect the general approach of the framework (e.g., not restricted to public authorities only). Furthermore, the commitment to implement the framework within the organization should be full and sincere. The contact points within the organization should be in the right position to influence and achieve the needed IT and risk management decisions and approaches that are associated with the framework at the corporate level. In what follows the main characteristics of the evaluation plan will be explained.

7.2 Evaluation Plan

In the following sections the description of the planning developed for each of the phases that make up the validation process of the proposed framework is presented.

7.2.1 Phase 1

It is planned that before the implementation of the framework, a group of stakeholders of each of the two organizations must complete one "Compliance evaluation sheet". The minimum set of subjects must complete that document is set to three persons: Chief Technology Officer (CIO) or similar role and two members of the team whose dedication to compliance management is deemed sufficient in terms of participation and criticality. The evaluation sheet adheres to the structure that is reflected in the following lines.

- **General data on participant**
  - Gender
  - Age
  - Role
  - Years of professional experience
  - Years of experience in the role
- **Compliance management**
  - Overall satisfaction with compliance management in CC (Very satisfied; Satisfied; Neither; Dissatisfied; Very dissatisfied).
  - Overall satisfaction with CC service (Very satisfied; Satisfied; Neither; Dissatisfied; Very dissatisfied).
  - Overall perception on the contribution of compliance management in CC to the quality of service of IT (Very High; Above Average; Average; Below Average; Very Low).
  - Overall perception on the contribution of compliance management in CC to the organizational compliance management process (Very High; Above Average; Average; Below Average; Very Low).

Additionally, a document must be filled out by CIO, Compliance Manager or similar role. The report, named "Compliance Metrics" collects data on project performance in relation to compliance by including several metrics on the topic.

- Average time lag between identification of external compliance issues and resolution.
- Number of compliance issues where employees seek guidance or assistance.
- Number of reports of alleged or actual Compliance violations.
- Percentage of compliance improvement opportunities implemented.
- Frequency (in days) of compliance reviews.

The doctoral student endured the encoding process reports through a process of assistance in person and as alternative methods adopted chat support, electronic-mail and telephone. Once he had all the information, he carried out a digitization of information for later analysis using a statistical software package.

Apart from that, in order to provide also a metric on the overall contribution to IT as a whole, a CMMI-based assessment is performed. In order to reach a certain maturity level, all control objective in a process area must be achieved, or mostly achieved with few remaining exceptions. The assessment of maturity levels is conducted over a longer period of time in order to better reflect the added value of the framework.

The maturity levels were obtained through self-assessments. The first round of assessments was conducted before the framework was introduced, the second one – twelve weeks after the framework was introduced.

The estimation of maturity levels was conducted as follows:

- Questions belonging to the specific maturity level are answered;
    - If all or most questions are answered positively then the questions belonging to the next higher maturity level are also answered;
    - If not, then the questions belonging to the next lower maturity level are also answered.
- This is repeated until all questions belonging to a certain maturity level are answered positively.

The self-assessments were conducted by internal experts of the organization. All had multiple years of experience as IT compliance managers, some were members of the IT risk management department, others of the IT compliance (having previous experience as managers in a multinational auditing company), and others were members of the internal revision. Two more employees of the evaluation partner were tasked with assessing the results of the evaluation for the purpose of the organization and continuing the activities beyond the scope of this thesis in the future.

7.2.2 Phase 2

Similarly to the provisions in the previous section, Phase 2 required the participants completing the same two reports. In order to ensure comparability of evaluation environments, the doctoral student endured the process of data acquisition and later codified the results for later analysis. This phase also included the CMMI-based assessment.

7.2.3 Phase 3

In this section, specific decisions on statistical analysis of the different phases are detailed. These analyses are performed over the same period of time as the conduction of the previous evaluations according to the specification of the analysis carried out in this section.

With regard to Phase 1 and Phase 2, a number of statistical tests have been applied. To know the mean scores and their standard deviations, a descriptive analysis of the variables was carried out. To find the relation of a set of variables to an independent variable, the ANOVA test has been applied to each parameter with a confidence interval of 95%. Finally, to establish the differences between two mean scores, Student's t-test was applied and the level of significance was set at $P < 0.05$.

Regarding Phase 3 or comparative analysis, the tests applied are the same as in previous phases.

7.3 Evaluation Execution

In this section, author describes the context of the execution of the validation performed in the three phases defined as well as the details of the execution of these phases.

7.3.1 Execution context

Three different phases have been established to evaluate the proposed framework. These three phases are different in their execution in time but also in the physical and operational context, the context of each one of them is described independently. In order to generate evaluation results that are both representative and reliable only partners with higher compliance requirements were considered during the selection of evaluation partners in industry. Furthermore, a proper mix of big and small organizations, of relevant business processes and of business-to-business (B2B) and B2C (business-to-customer) scenarios was aimed at. Thus, two case studies were selected.

7.3.1.1 Case Study 1

The first evaluation partner is a leading insurance company from Germany (Top 5) that operates throughout Germany and offers a full range of insurance services to its clients. The company is particularly strong in the insurance business with private customers thus emphasizing the B2C aspect as already suggested.

First talks about a possible evaluation with the partner started as soon as the idea of the framework was structured at the beginning of 2015. As part of the assessment of the organization as a possible evaluation partner the relevant requirements of the organization were solicited, including its structure, its management systems, its projects, the relevant legal aspects, as well as findings from current risk audits and assessments conducted in the organization by KPMG. Following this, an analysis of the existing communication interfaces was conducted.

The interface between the different business units and the internal IT services company was identified as the best organizational area to implement the framework. It represents a very good match with the communication paradigms assumed by the framework.

As of May 2015 the organization reported a general agreement to implement the framework in the near future and named the following pain points that they expected the framework to address:

- Rising costs of IT compliance due to a missing IT compliance function in the organization, and
- High risks associated with non-compliance that currently cannot be quantified.

The objectives that the organization aimed to achieve by adopting the framework were the following:

- Avoidance of “conformity-gaps” between requirements and their actual implementation in IT,
- Implementation of changes in a holistic, risk-oriented consideration of IT compliance,
- Central governance of requirements and a higher degree of standardization during implementation (increase in maturity levels),
- Assurance of compliant IT operations, e.g. by closing existing non-compliance findings and a proven compliance with existing regulations, and
- Reduction of the likelihood of occurrence and the potential damage of risks.

The actual evaluation started in the second half of 2015 with the assessment of the status-quo of the areas that the framework would affect (Phase 1). This was needed in order to have detailed view of the situation before the framework is introduced within the organization. Furthermore, it was assessed how the framework should be tailored to the specifics of the organization in order to reflect its structure, business processes, paradigms and priorities.

After completion of this assessment the actual implementation of the framework started at the beginning of 2016. In the first three months of 2016 the framework was implemented within the organization with the objective to implement at least 70% of the framework elements that were identified during the customization.

7.3.1.2 Case Study 2

The second partner is an IT service provider that offers a range of IT services to institutional customers only. Thus, it is emphasizing the B2B aspect in the evaluation.

Preliminary talks about a possible evaluation with the partner started as soon as the idea of the framework was structured at the beginning of 2015. As part of the assessment of the organization as a possible evaluation partner the relevant requirements of the organization were solicited, including its structure, its management systems, its projects, the relevant legal aspects, as well as findings from current internal risk audits and assessments conducted in the organization. Following this, an analysis of the existing communication interfaces was conducted.

The interface between external business clients and the IT services company itself was identified as the best organizational area to implement the framework. It represents a fairly good match with the communication paradigms assumed by the framework.

As of September 2015 the organization reported a general agreement to implement the framework in the near future and named the following pain points that they expected the framework to address:

- Better ability to articulate own IT compliance to existing and potential customers, and
- Ensuring compliance of IT operations for customers with highest requirements, e.g. defense and intelligence agencies.

The objectives that the organization aimed to achieve by adopting the framework were the following:

- Avoidance of "conformity-gaps" between requirements and their actual implementation in IT,
- Implementation of changes in a holistic, risk-oriented consideration of IT compliance,
- Definition of service levels with respect to compliance that apply to offerings for different customer segments,
- Central governance of requirements for every customer segment and a higher degree of standardization in the offerings (increase in maturity levels),
- Assurance of compliant IT operations, e.g. by closing existing non-compliance findings and a proven compliance with existing regulations, and
- Reduction of the likelihood of occurrence and the potential damage of risks.

The actual evaluation started at the beginning of 2016 with the assessment of the status-quo of the areas that the framework would affect (Phase 1). This was needed in order to have detailed view of the situation before the framework is introduced within the organization. Furthermore, it was assessed how the framework should be tailored to the specifics of the organization in order to reflect its structure, business processes, paradigms and priorities.

After completion of this assessment the actual implementation of the framework started in April 2016. In the three months afterwards the framework was implemented within the organization with the objective to implement at least 80% of the framework elements that were identified during the customization.

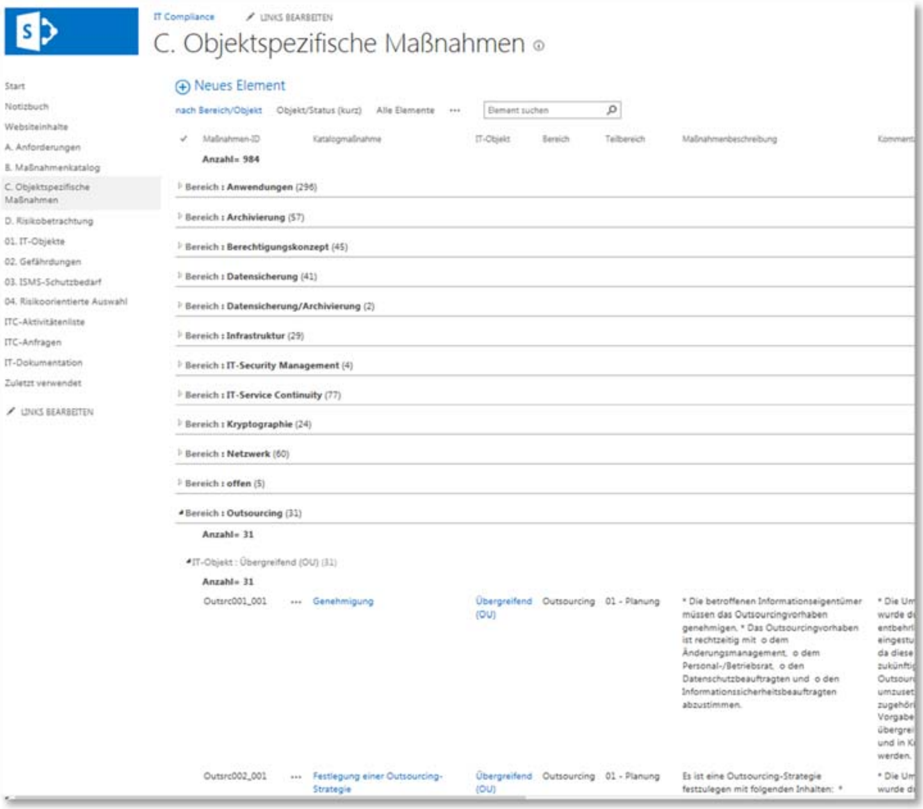
7.3.2 Evaluation Phases Execution

In the following sections main internals about the execution of the different phases defined in the evaluation of the framework in each of the two case studies executed are explained.

7.3.2.1 Case Study 1

One of the most important tasks to be performed before the execution of the framework was the customization of the framework to the specific needs of the organization.

The customization of the framework for Evaluation Partner 1 was conducted in close collaboration with the partner. As already stated, the customization aimed to reflect the specific expectations and objectives of the partner as stated earlier. Due to the geographically distributed project team at the evaluation partner and the multiple sites where the framework was implemented the customization was supported by the use of MS SharePoint (Figure 15).



C. Objektspezifische Maßnahmen

✓	Maßnahmen-ID		Katalogmaßnahme	IT-Objekt	Bereich	Teilbereich	Maßnahmenbeschreibung	Komment
	Anzahl= 984							
Bereich : **Anwendungen** (296)								
Bereich : **Archivierung** (57)								
Bereich : **Berechtigungskonzept** (45)								
Bereich : **Datensicherung** (41)								
Bereich : **Datensicherung/Archivierung** (2)								
Bereich : **Infrastruktur** (29)								
Bereich : **IT-Security Management** (4)								
Bereich : **IT-Service Continuity** (77)								
Bereich : **Kryptographie** (24)								
Bereich : **Netzwerk** (60)								
Bereich : **offen** (5)								
Bereich : **Outsourcing** (31)								
	Anzahl= 31							
IT-Objekt : Übergreifend (OU) (31)								
	Anzahl= 31							
	Outsrc001_001	•••	Genehmigung	Übergreifend (OU)	Outsourcing	01 - Planung	* Die betroffenen Informationseigentümer müssen das Outsourcingvorhaben genehmigen. * Das Outsourcingvorhaben ist rechtzeitig mit o dem Änderungsmanagement, o dem Personal-/Betriebsrat, o den Datenschutzbeauftragten und o den Informationssicherheitsbeauftragten abzustimmen.	* Die Um wurde d entbehrl eingestu da diese zukünftig Outsour umzuset zugehöri Vorgabe übergrei und in K werden.
	Outsrc002_001	•••	Festlegung einer Outsourcing-Strategie	Übergreifend (OU)	Outsourcing	01 - Planung	Es ist eine Outsourcing-Strategie festzulegen mit folgenden Inhalten: *	* Die Um wurde d

Figure 15. A View of the MS SharePoint Portal that was used during Framework Customization with Evaluation Partner 1

The following methodological customizations were applied:

- Customization of the protection requirement categories,
- Substitution of certain values that could not be assessed in the organization a-priori with assumptions,
- Extension of the framework to all IT areas (not only cloud services or outsourcing),
- Agreement on the usage of maturity levels as aggregate indicators for the frameworks performance, and
- Development of the tool support by MS SharePoint not only for the customization but also for the actual evaluation of the framework.

Thus the customization assured that the framework reflects the objectives and paradigms of the organization which in turn led to a higher level of commitment of the organization.

As reported earlier, first talks about a possible evaluation with the partner started as soon as the idea of the framework was structured at the beginning of 2015. As of May 2015 the organization reported a general agreement to implement the framework. Phase 1 took place in the second half of 2015 and Phase 2 started by started in March 2016.

7.3.2.2 Case Study 2

Again, there is a need to perform the customization of the framework to the specific needs of the organization before its execution. The customization of the framework for Evaluation Partner 2 was also conducted in close collaboration with the partner. Here too, the customization aimed to reflect the specific expectations and objectives of the partner as stated previously. In this case, the project team was present at the same geographic location (Berlin, Germany). Thus, the main parts of the interaction were conducted in presence of the stakeholders and not remotely.

As stated before, preliminary talks about a possible evaluation with the partner started as soon as the idea of the framework was structured at the beginning of 2015. As of September 2015 the organization reported a general agreement to implement the framework. Phase 1 took place in beginning of 2016 and Phase 2 started by started in April 2016.

7.4 Analysis

The evaluation of this thesis aims to demonstrate that the resulting framework will improve existing approaches within the research community and industry with respect to risk assessment, including accuracy, completeness and performance of defined controls. The use of real-life examples from existing organizations with elaborate management systems should establish the comparative environment for the evaluation of the framework as a newly-designed artefact.

The following sections deal with the description of the data and the subsequent analysis of the data corresponding to the execution of phases 1 to 3.

7.4.1 Phase 1

In what follows, details on the data collected for both case studies before the implementation of the framework are presented.

7.4.1.1 Case Study 1

Each case study provides two different sources of information. Firstly, the one gathered by means of the two previously described questionnaires and secondly, the CMMI-based evaluation. These two sets are described in the following lines:

7.4.1.1.1 Questionnaires

COMPLIANCE EVALUATION SHEET

A total of 11 respondents answered the questionnaire. Regarding the sample it is composed by 2 female respondents (18.18%) and 9 male (81.82%). Three different roles are represented in the sample: CIO (9.09%), Manager (36.36%) and Group Leader (54.55%) as depicted in the following figure:

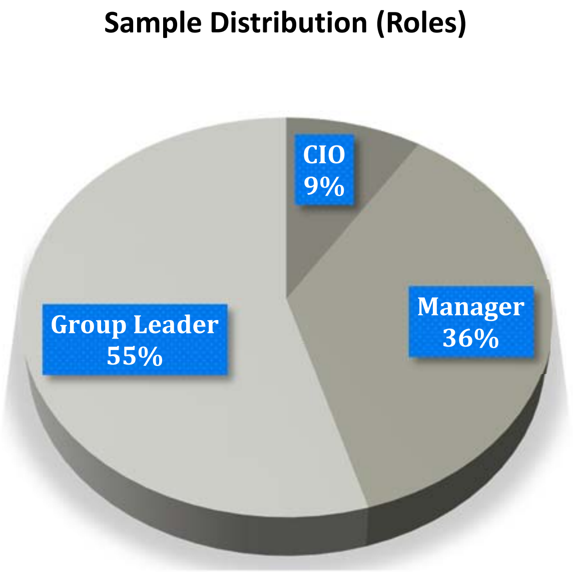


Figure 16. Distribution of roles among the sample in Phase 1 Case Study 1

Average age is 36.09 years old, average years of professional experience is 11.55 years and average experience in the current role is 4.36 years. Regarding the four specific questions labelled using a Likert scale, the distribution of responses with regards to the satisfaction on Compliance Management in CC, this is as follows:

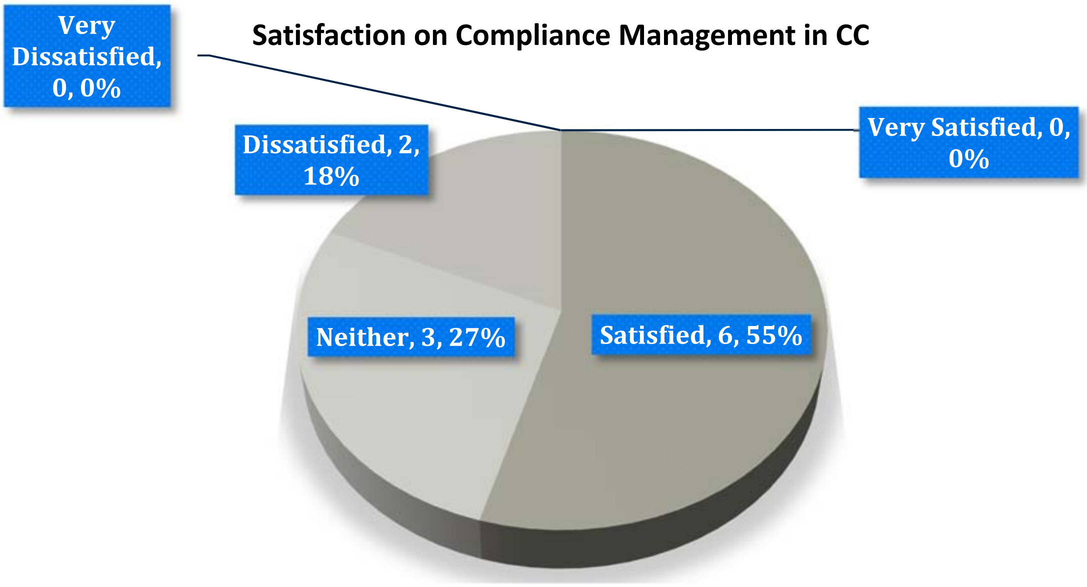


Figure 17. Satisfaction Compliance Management in CC. Phase 1 of Case Study 1

As pictured in the previous figure, most of the respondents felt satisfied with compliance management (55%) while 27% remain neutral on the topic. Just 2 respondents are dissatisfied and there are not extreme values in the sample.

With regards to the Satisfaction on the CC service in the organization, distribution and answers are coded in the following figure:

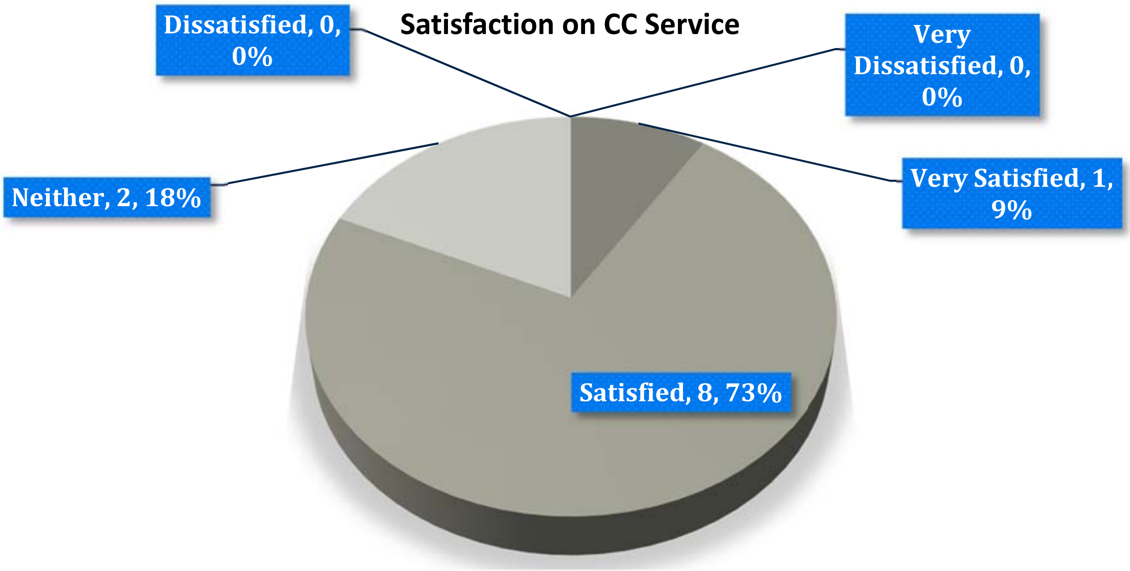


Figure 18. Satisfaction on CC Service. Phase 1 of Case Study 1

As pictured in the previous figure, most of the respondents felt satisfied with CC service (73%) or very satisfied (9%) with it, while 18% remained neutral on the topic. There are not negative values coded by respondents.

With regard to the contribution of compliance management in CC to IT quality of service, distribution and answers are coded in the following figure:

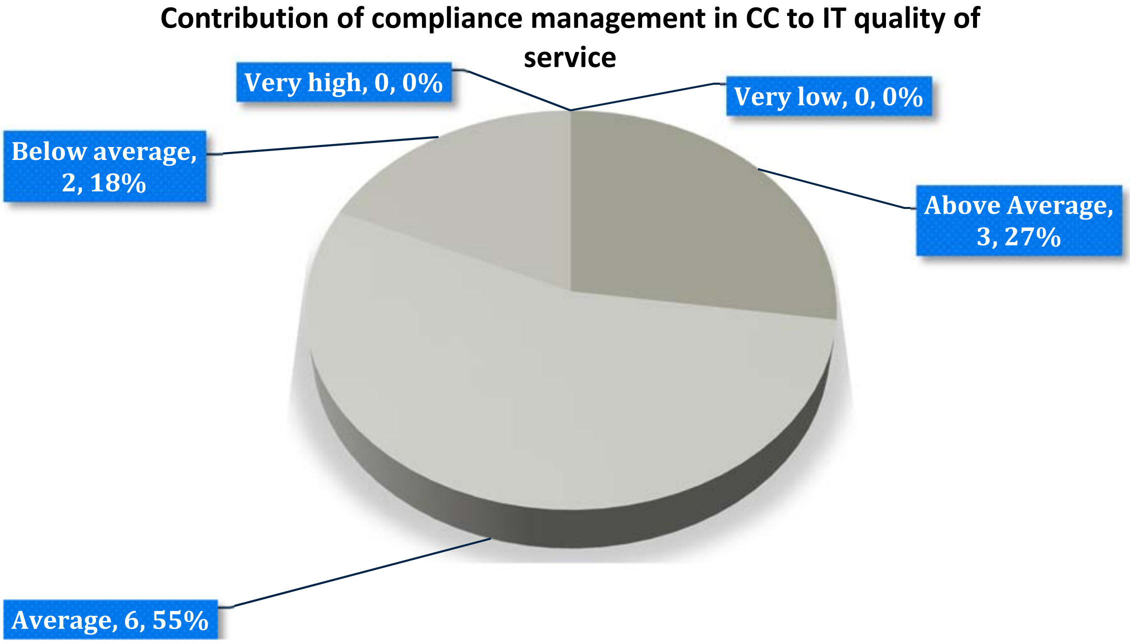


Figure 19. Contribution of compliance management in CC to IT quality of service. Phase 1 of Case Study 1

Respondents believe the current contribution of compliance management in cloud computing to IT quality of service is average in most cases (55%), while in 27% of the cases it is above average and 18% of the cases is below average.

The last piece of information taken from the questionnaire is the opinion on the contribution of compliance management in the field of CC to the corporate compliance management. This is presented in the following figure:

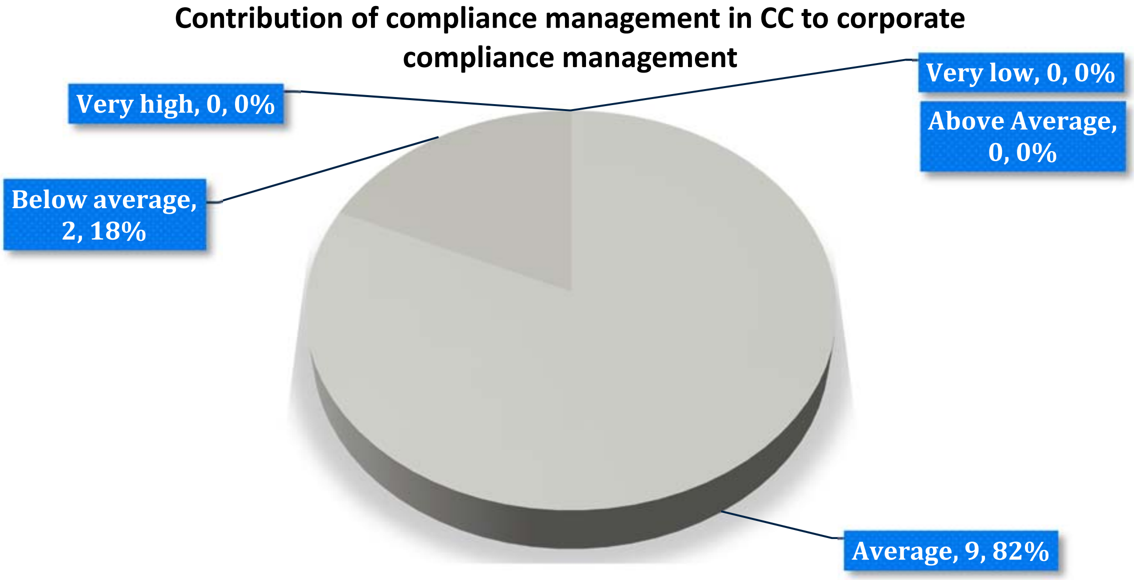


Figure 20. Contribution of compliance management in CC to corporate compliance management. Phase 1 of Case Study 1

Again, respondents provided quite central responses. They believe the current contribution of compliance management in cloud computing to corporate compliance management is average in most cases (82%), while in 18% of the cases it is below average.

To sum up data obtained, the following table gathers numeric information about respondents coding Likert scales (1-5) with their corresponding values by providing their statistical descriptions. In the table Mean (M) and Standard Deviation (SD) of the different variables is provided:

Table 17. Compliance evaluation sheet. Phase 1 of Case Study 1

	M	SD
Satisfaction CC service	3.91	.539
Satisfaction compliance management in CC	3.36	.809
Contribution compliance management in CC to IT quality of service	3.09	.701
Contribution compliance management in CC to the organizational compliance management	2.82	.405

Regarding the first variable, the overall satisfaction with the CC service is quite high (3.91) and the dispersion is very limited according to the standard deviation. It is worth to note that the overall satisfaction with the compliance management aspect is quite high (3.36), but also it is important to take into account that the standard deviation is the highest among the variables (.809), showing a remarkable dispersion. The third variable is the contribution of compliance management to the overall IT quality of service. This aspect is quite moderate according to its mean (3.09) and also presents a relatively high dispersion (.701) showing the somewhat unclear importance of compliance management to IT quality of service. Finally, the contribution of compliance management to the overall compliance management presents the lowest score around (2.82) and the dispersion is also the lowest (.405). This circumstance is maybe connected to the fact that the organization in Case 1 presents a complex compliance scenario in which CC matters are not too important compared to the overall compliance scenario.

The second step in the analysis is the comparison of results among roles. The aim is to compare opinions to check for differences among roles. In Case Study 1, just three roles are presented namely CIO, Manager and Group Leader. In order to know if there are statistical differences among roles, the ANOVA test has been applied. Results show there are no significant statistical differences among groups in variables studied. The following table summarizes results obtained for the variables studied:

Table 18. ANOVA results among roles. Phase 1 of Case Study 1

	ANOVA
Satisfaction CC service	F(10)=.304, p>0,05
Satisfaction compliance management in CC	F(10)=.107, p>0,05
Contribution compliance management in CC to IT quality of service	F(10)=1.480, p>0,05
Contribution compliance management in CC to the organizational compliance management	F(10)=.134, p>0,05

However, there is a need to know if there are statistical significant differences between roles analysed in pairs. Using the Student's t-test, we obtained the mean differences between variables group in pairs. The following table presents Student T test results of the comparison between CIOs and Managers.

Table 19. Student T test results between CIO and Manager. Phase 1 of Case Study 1

	Student T test
Satisfaction CC service	t (4)=.701, p>0,05
Satisfaction compliance management in CC	t (4)=.000, p>0,05
Contribution compliance management in CC to IT quality of service	t (4)=.701, p>0,05

Contribution compliance management in CC to the organizational compliance management	t (4)=.447, p>0,05

According to data provided, there are no statistical differences between populations. The following table presents Student T test results of the comparison between CIOs and Group Leaders.

Table 20. Student T test results between CIO and Group Leaders. Phase 1 of Case Study 1

	Student T test
Satisfaction CC service	t (6)=.378, p>0,05
Satisfaction compliance management in CC	t (6)=.756, p>0,05
Contribution compliance management in CC to IT quality of service	**t (6)=2.646, p<0,05**
Contribution compliance management in CC to the organizational compliance management	t (6)=.378, p>0,05

The only significant statistical difference found is the third variable in which CIOs and Groups leaders present different opinions on the contribution of compliance management in CC to the overall IT Quality of service. This is quite an interesting finding that will be discussed in the following sections. The following table presents Student T test results of the comparison between Managers and Group Leaders.

Table 21. Student T test results between Managers and Group Leaders. Phase 1 of Case Study 1

	Student T test
Satisfaction CC service	t (9)=-.434, p>0,05
Satisfaction compliance management in CC	t (9)=-.148, p>0,05
Contribution compliance management in CC to IT quality of service	t (9)=.964, p>0,05
Contribution compliance management in CC to the organizational compliance management	t (9)=-.290, p>0,05

Once more, according to data provided, there are not statistical differences between populations.

COMPLIANCE METRICS

The second questionnaire was circulated among CIOs or similar roles in the two companies. In the following table, main figures for the five KPIs are presented:

Table 22. Main Compliance Metrics. Phase 1 of Case Study 1

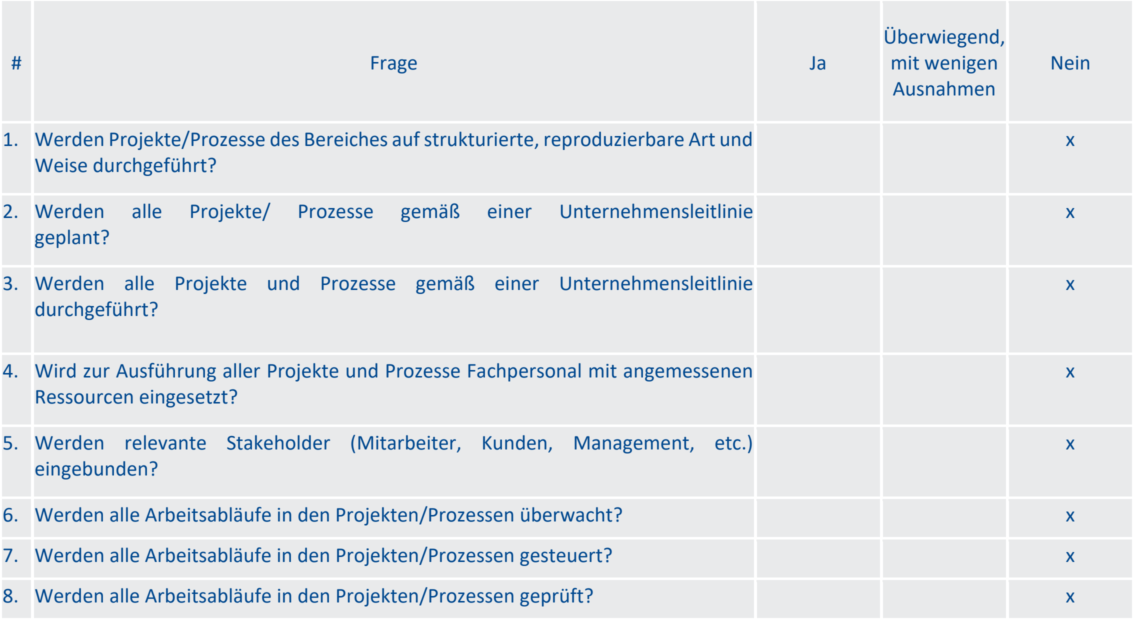
Metric	Value
Average time lag between identification of external compliance issues and resolution	48
Number of compliance issues where employees seek guidance or assistance	19
Number of reports of alleged or actual Compliance violations	89
Percentage of compliance improvement opportunities implemented	73
Frequency (in days) of compliance reviews	60

As depicted in the previous table, metrics were collected before the implementation of the framework in order to be later analysed comparing data recorded in Phase 1 and Phase 2. Analysis will be performed in the Phase 3.

7.4.1.1.2 CMMI Based Evaluation

The first round of assessments – before the implementation of the framework – was finished at the beginning of 2016 for Case Study 1. There, a maturity level of one was estimated, as all questions related to maturity level two were answered negatively (Table 23).

Table 23. Answered Questions related to Maturity Level 2 before Framework Introduction (in German)



#	Frage	Ja	Überwiegend, mit wenigen Ausnahmen	Nein
1.	Werden Projekte/Prozesse des Bereiches auf strukturierte, reproduzierbare Art und Weise durchgeführt?			x
2.	Werden alle Projekte/ Prozesse gemäß einer Unternehmensleitlinie geplant?			x
3.	Werden alle Projekte und Prozesse gemäß einer Unternehmensleitlinie durchgeführt?			x
4.	Wird zur Ausführung aller Projekte und Prozesse Fachpersonal mit angemessenen Ressourcen eingesetzt?			x
5.	Werden relevante Stakeholder (Mitarbeiter, Kunden, Management, etc.) eingebunden?			x
6.	Werden alle Arbeitsabläufe in den Projekten/Prozessen überwacht?			x
7.	Werden alle Arbeitsabläufe in den Projekten/Prozessen gesteuert?			x
8.	Werden alle Arbeitsabläufe in den Projekten/Prozessen geprüft?			x

9.	Wird die Einhaltung der Projekt-/Prozessbeschreibungen bewertet?			x
10.	Ist der Zustand der Arbeitsergebnisse für das Management an definierten Punkten sichtbar (zum Beispiel Meilensteine)?			x
11.	Werden verpflichtende Inputs relevanter Stakeholder etabliert?			x
12.	Werden verpflichtende Inputs relevanter Stakeholder bedarfsgerecht überarbeitet?			x
13.	Werden die Arbeitsergebnisse angemessen gelenkt?			x
14.	Erfüllen die Arbeitsergebnisse die spezifizierten Prozessbeschreibungen, Normen und Verfahren?			x

7.4.1.2 Case Study 2

As indicated in the first case study, each case study provides two different sources of information. Firstly, the one gathered by means of the two previously described questionnaires and secondly, the CMMI based evaluation. Again, these two sets are described in the following lines in the scenario provided before the implementation of the framework:

7.4.1.2.1 Questionnaires

COMPLIANCE EVALUATION SHEET

A total of 10 respondents answered the questionnaire. Regarding the sample it is composed by 1 female respondent (10%) and 9 male (90%). Four different roles are represented in the sample: CIO (10%), Vice-president (10%), Manager (20%) and Group Leader (60%) as depicted in the following figure:

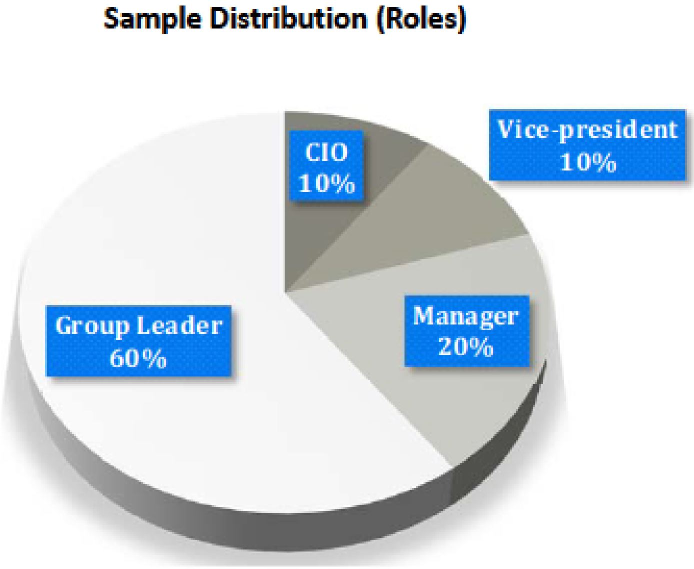


Figure 21. Distribution of roles among the sample in Phase 1 of Case Study 2

Average age is 37.40 years old, average years of professional experience is 14.20 years and average experience in the current role is 7 years. Regarding the four specific questions labelled using a Likert scale, the distribution of responses with regards to the satisfaction on Compliance Management in CC, this is as follows:

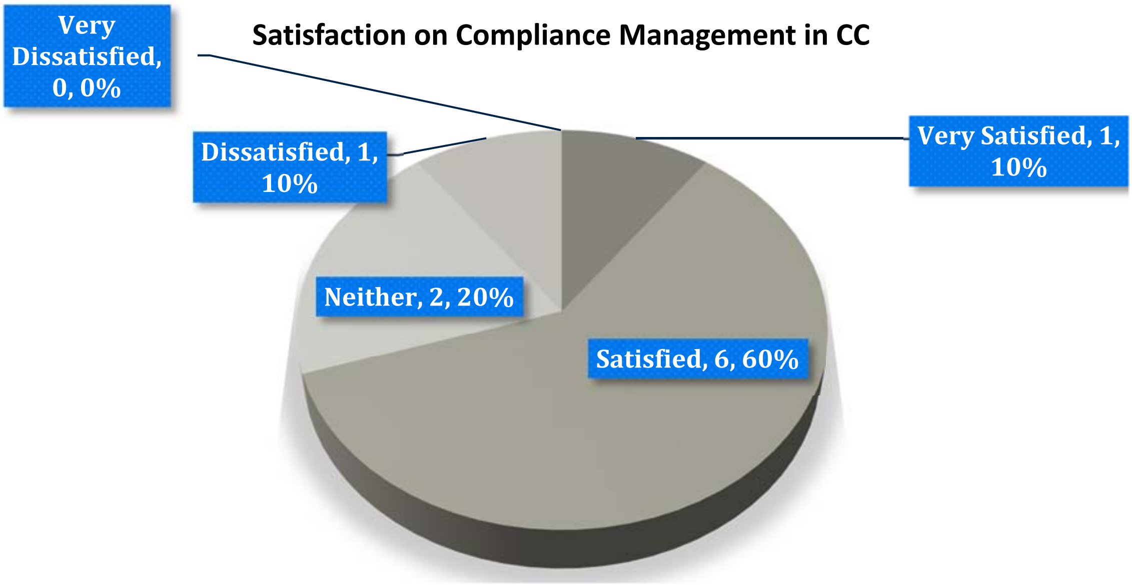


Figure 22. Satisfaction Compliance Management in CC. Phase 1 of Case Study 2

As pictured in the previous figure, most of the respondents felt satisfied with compliance management (60%), while one more respondent felt Very Satisfied while 20% remain neutral on the topic. Just one respondent is dissatisfied and there are no subjects Very Dissatisfied in the sample.

With regard to the Satisfaction on the CC service in the organization, distribution and answers are coded in the following figure:

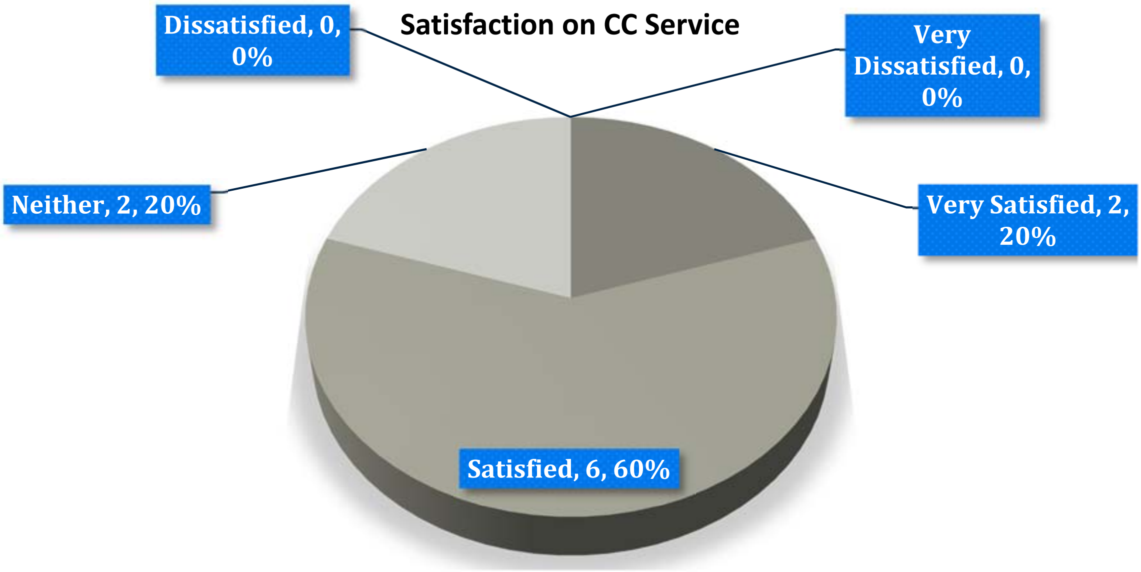


Figure 23. Satisfaction on CC Service. Phase 1 of Case Study 2

As pictured in the previous figure, most of the respondents felt satisfied with CC service (60%) or very satisfied (20%) with it, while 20% remain neutral on the topic. There are no negative values coded by respondents.

With regards to the contribution of compliance management in CC to IT quality of service, distribution and answers are coded in the following figure:

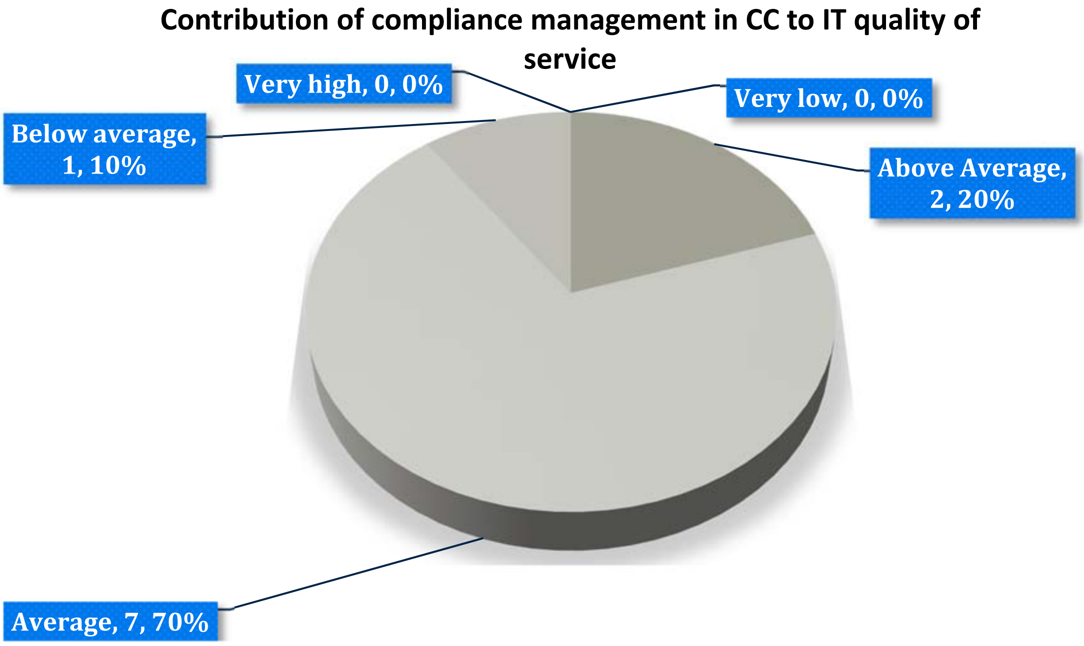


Figure 24. Contribution of compliance management in CC to IT quality of service. Phase 1 of Case Study 2

Respondents believe the current contribution of compliance management in cloud computing to IT quality of service is average in most cases (70%), while in 20% of the cases it is above average and in 10% of the cases is below average.

The last piece of information taken from the questionnaire is the opinion on the contribution of compliance management in the field of CC to the corporate compliance management. This is presented in the following figure:

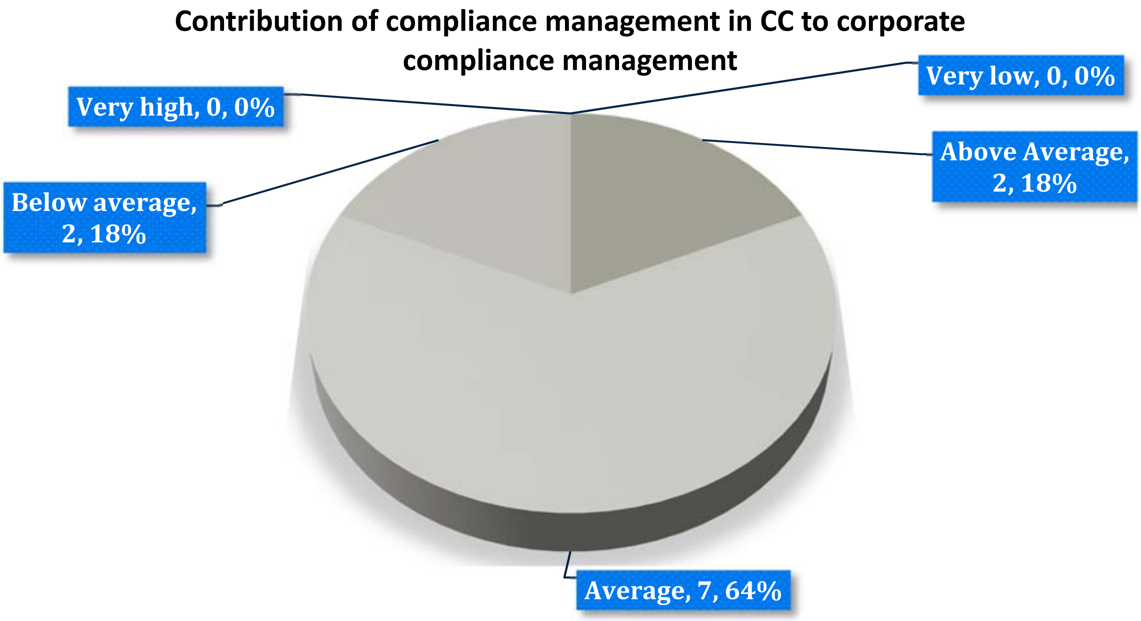


Figure 25. Contribution of compliance management in CC to corporate compliance management. Phase 1 of Case Study 2

Again, respondents provided quite central responses. They believe the current contribution of compliance management in cloud computing to corporate compliance management is average in most cases (70%), while in 20% of the cases it is above average and just 10% is below average.

Following the approach adopted for Case study 1, the following table gathers numeric information about respondents coding Likert scales (1-5) with their corresponding values by providing their statistical descriptions. In the table Mean (M) and Standard Deviation (SD) of the different variables are provided:

Table 24. Compliance evaluation sheet. Phase 1 of Case Study 2

	M	SD
Satisfaction CC service	4.00	.667

Satisfaction compliance management in CC	3.70	.823
Contribution compliance management in CC to IT quality of service	3.10	.568
Contribution compliance management in CC to the organizational compliance management	3.10	.568

Regarding the first variable, the overall satisfaction with the CC service is quite high (4.00) and the dispersion is higher than before, according to the standard deviation (.667). It is worth to note that the overall satisfaction with the compliance management aspect is quite high (3.70), but also it is important to take into account that the standard deviation is, again, the highest among the variables (.823), showing a remarkable dispersion. The third variable is the contribution of compliance management to the overall IT quality of service. This aspect is quite moderate according to its mean (3.10) and also presents a moderate dispersion (.568) showing the pale importance of compliance management to IT quality of service. Finally, the contribution of compliance management to the overall compliance management presents same figures obtained for the previous variable (3.10) and the dispersion is also moderate(.568). This could be caused by the fact that the organization in Case 2 is devoted to IT and the overall compliance management can be identified as the IT compliance management and the quality of IT is finally connected with its conformance.

The second step in the analysis is the comparison of results among roles. The aim is to compare opinions to check for differences among roles. In Case Study 2, just three roles are presented namely CIO (In this category we add also Vice-president to be consistent with Case 1), Manager and Group Leader. In order to know if there are statistical differences among roles, the ANOVA test has been applied. Results show there are no significant statistical differences among groups in three of the four variables studied. In the case of the Satisfaction with CC service there are statistical significant differences. This is caused by the opinions given by top managers labelling their satisfaction on the service as very high. The following table summarizes results obtained for the variables studied:

Table 25. ANOVA results among roles. Phase 1 of Case Study 2

	ANOVA
Satisfaction CC service	**F(9)=7.000, p<0,05**
Satisfaction compliance management in CC	F(9)=1.244, p>0,05
Contribution compliance management in CC to IT quality of service	F(9)=.560, p>0,05

Contribution compliance management in CC to the organizational compliance management	F(9)=.560, p>0,05

However, there is a need to know if there are statistical significant differences between roles analysed in pairs. Using the Student's t-test, we obtained the mean differences between variables group in pairs. The following table presents Student T test results of the comparison between CIOs and Managers.

Table 26. Student T test results between CIOs and Managers. Phase 1 of Case Study 2

	Student T test
Satisfaction CC service	t (3)=1.000, p>0,05
Satisfaction compliance management in CC	t (3)=1.414, p>0,05
Contribution compliance management in CC to IT quality of service	t (3)=1.000, p>0,05
Contribution compliance management in CC to the organizational compliance management	t (3)=1.000, p>0,05

According to data provided, there are no statistical differences between populations. The following table presents Student T test results of the comparison between CIOs and Group Leaders.

Table 27. Student T test results between CIO and Group Leaders. Phase 1 of Case Study 2

	Student T test
Satisfaction CC service	**t (7)=3.464, p<0,05**
Satisfaction compliance management in CC	t (7)=1.500, p>0,05
Contribution compliance management in CC to IT quality of service	t (7)=.949, p>0,05
Contribution compliance management in CC to the organizational compliance management	t (7)=.949, p>0,05

The only significant statistical difference found is the first variable in which CIOs and Groups leaders present different opinions on the satisfaction of CC service. As stated before in the ANOVA test, this is due to the high satisfaction perceived by top managers. The following table presents Student T test results of the comparison between Managers and Group Leaders.

Table 28. Student T test results between Managers and Group Leaders. Phase 1 of Case Study 2

	Student T test
Satisfaction CC service	t (7)=-.866, p>0,05
Satisfaction compliance management in CC	t (7)=-.000, p>0,05
Contribution compliance management in CC to IT quality of service	t (7)=.000, p>0,05
Contribution compliance management in CC to the organizational compliance management	t (7)=-.000, p>0,05

Once more, according to data provided, there are no statistical differences between populations.

COMPLIANCE METRICS

The second questionnaire was circulated among CIOs or similar roles in the two companies. In the following table, main figures for the five KPIs are presented:

Table 29. Main Compliance Metrics. Phase 1 of Case Study 2

Metric	Value
Average time lag between identification of external compliance issues and resolution.	36
Number of compliance issues where employees seek guidance or assistance.	12
Number of reports of alleged or actual Compliance violations.	75
Percentage of compliance improvement opportunities implemented.	76
Frequency (in days) of compliance reviews.	30

Again, as depicted in the previous table, metrics were collected before the implementation of the framework in order to be later analysed comparing data recorded in Phase 1 and Phase 2.

7.4.1.2.2 CMMI Based Evaluation

The first round of assessments – before the implementation of the framework – was finished by March of 2016. There, a maturity level of one was estimated for all areas that were defined as relevant during the framework customization with evaluation partner 2 (Table 30). Here again, the technology-oriented view of evaluation partner 2 is clearly reflected in the areas.

Table 30. Question Areas and their Maturity Levels before Framework Introduction at Partner 2 / Case Study 2

Area	Maturity Level at t=0
network	1
applications	1
authorization concept	1
anti-virus	1
cryptography	1
patch-/change-management	1
archiving and backup	1
infrastructure	1
logging	1

7.4.1.3 Overall comparison

In the following section the analysis performed to compare results obtained in both case studies are depicted, particularizing the analysis in the two instruments circulated to obtain data for the Phase.

7.4.1.3.1 Compliance Evaluation Sheet

Following the approach adopted earlier, we will start the analysis presenting descriptive statistics of previous phases. In the table, Mean (M) and Standard Deviation (SD) of the different variables are provided:

Table 31. Descriptive statistics on compliance evaluation sheet. Phase 1, overall comparison

	CASE 1		CASE 2	
	M	SD	M	SD
Satisfaction CC service	3.91	.539	4.00	.667
Satisfaction compliance management in CC	3.36	.809	3.70	.823
Contribution compliance management in CC to IT quality of service	3.09	.701	3.10	.568
Contribution compliance management in CC to the organizational compliance management	2.82	.405	3.10	.568

In general, it is worth to note that means and standard deviations are, in both cases, comparable. However, in all cases figures in means are higher in Case 2 compared to Case 1, although the differences are slender. Standard deviations are also analogous in all variables.

The second step in the analysis is the comparison of results between cases. Using the Student's t-test, we obtained the mean differences between variables obtained in both case studies. The following table presents Student T test results of the comparison between case studies 1 and 2 in Phase 1 for the four variables.

Table 32. Student T test results between case studies. Phase 1, overall comparison

	Student T test
Satisfaction CC service	t (20)=-.345, p>0,05
Satisfaction compliance management in CC	t (20)=-944, p>0,05
Contribution compliance management in CC to IT quality of service	t (20)=-032, p>0,05
Contribution compliance management in CC to the organizational compliance management	t (20)=-1.320, p>0,05

According to data provided, there are no statistical differences between case studies for this Phase 1. This means that data is comparable between cases.

7.4.1.3.2 Compliance Metrics Questionnaire

In the following table the two sets of data are presented with regards to the compliance metrics questionnaire:

Table 33. Compliance Metrics, Phase 1, overall comparison

Metric	Case 1	Case 2
Average time lag between identification of external compliance issues and resolution	48	36
Number of compliance issues where employees seek guidance or assistance	19	12
Number of reports of alleged or actual Compliance violations	89	75
Percentage of compliance improvement opportunities implemented	73	76
Frequency (in days) of compliance reviews	60	30

Again, data is quite comparable given the different backgrounds of the two organizations. Thus, there are metrics quite comparable (Average time lag between identification of external compliance issues and resolution, number of compliance issues where employees seek guidance or assistance, Number of reports of alleged or actual Compliance violations and Percentage of compliance improvement opportunities implemented) while the last metric, that depends on the current compliance management process and not the results of it, Frequency (in days) of compliance reviews, is different. However and in general, both organizations present similar data.

7.4.2 Phase 2

In what follows, details on the data collected for both case studies after the implementation of the framework are presented.

7.4.2.1 Case Study 1

As indicated in Phase 1, each case study provides two different sources of information. Firstly, the one gathered by means of the two previously described questionnaires and secondly, the CMMI based evaluation. Yet again, these two sets are described in the following lines in the scenario drawn after the implementation of the framework:

7.4.2.1.1 Questionnaires

COMPLIANCE EVALUATION SHEET

In Phase 2, same respondents answered the questionnaire, so sample composition and characteristics are the same as already explained in Phase 1. Regarding the four specific questions labelled using a Likert scale, the distribution of responses with regard to the satisfaction on Compliance Management in CC, this is as follows:

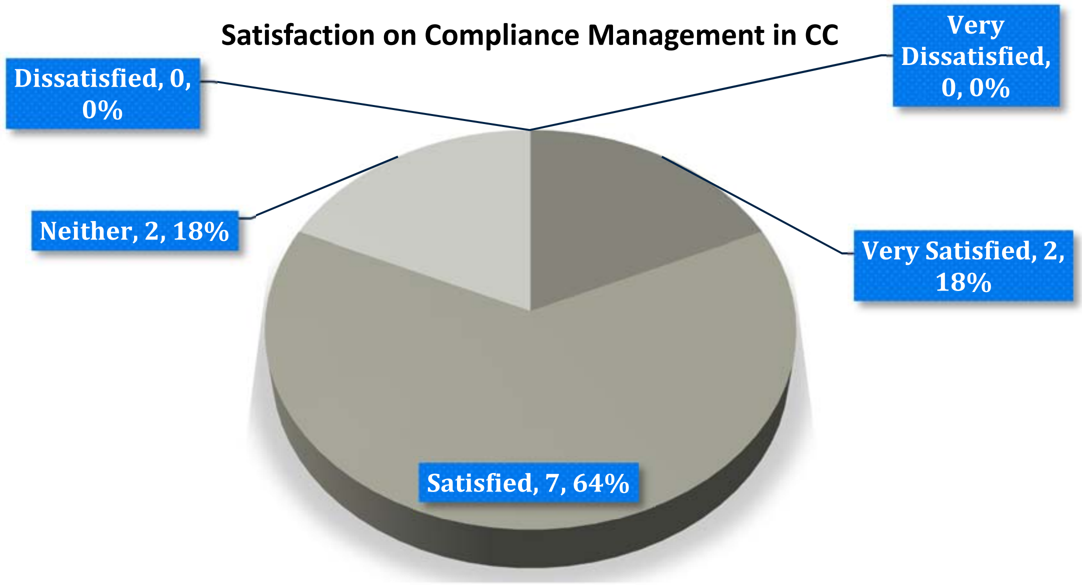


Figure 26. Satisfaction Compliance Management in CC. Phase 2 of Case Study 1

As pictured in the previous figure, most of the respondents felt satisfied with compliance management (64%) or very satisfied (18%) while 18% remain neutral on the topic. No respondents are dissatisfied after the implementation of the framework.

With regards to the Satisfaction on the CC service in the organization, distribution and answers are coded in the following figure:

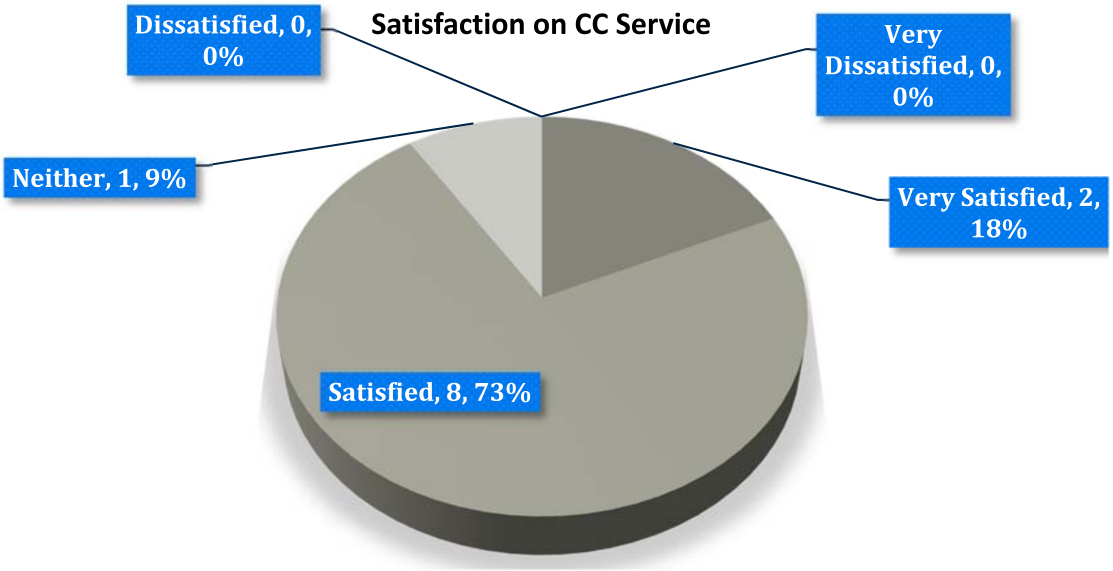


Figure 27. Satisfaction on CC Service. Phase 2 of Case Study 1

As pictured in the previous figure, most of the respondents felt satisfied with CC service (73%) or very satisfied (18%) with it, while 9% remain neutral on the topic. There are no negative values coded by respondents.

With regards to the contribution of compliance management in CC to IT quality of service, distribution and answers are coded in the following figure:

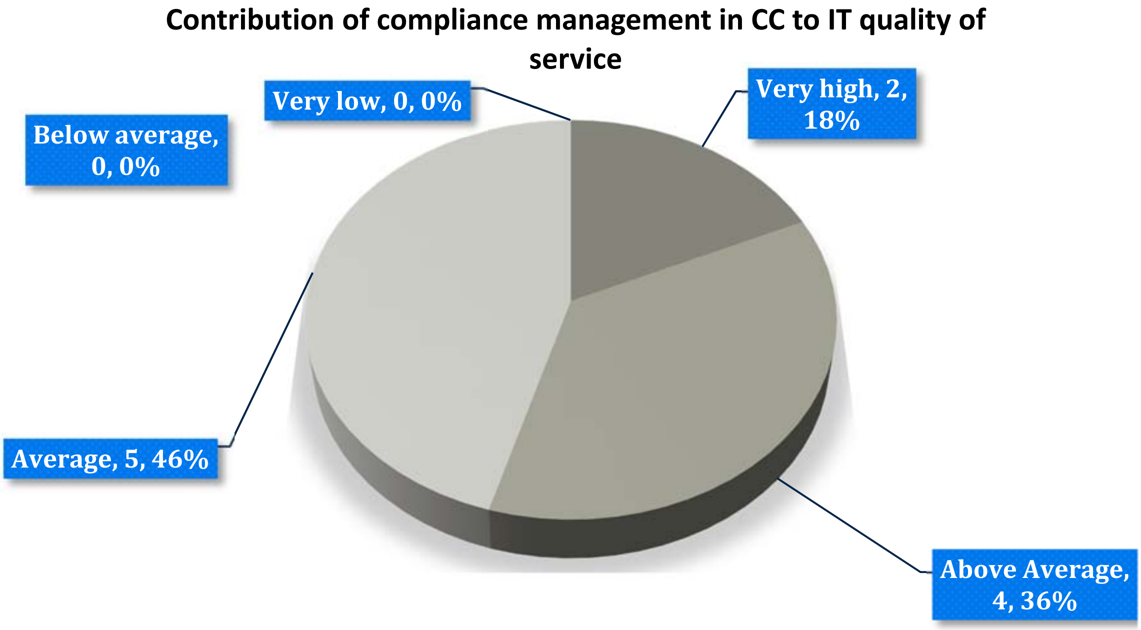


Figure 28. Contribution of compliance management in CC to IT quality of service. Phase 2 of Case Study 1

Respondents believe the current contribution of compliance management in cloud computing to IT quality of service is average (46%), while in 36% of the cases it is above average and 18% of the cases it is very high.

The last piece of information taken from the questionnaire is the opinion on the contribution of compliance management in the field of CC to the corporate compliance management. This is presented in the following figure:

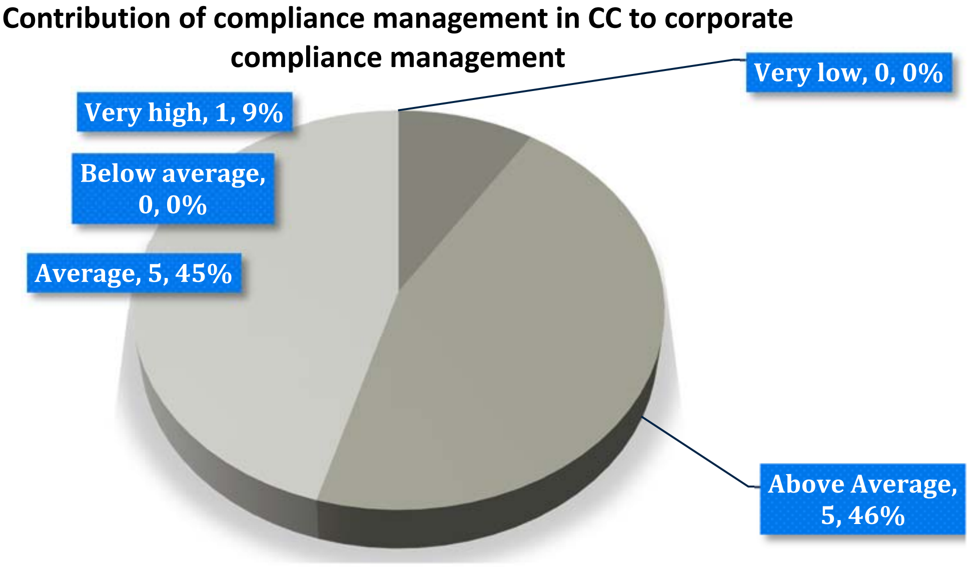


Figure 29. Contribution of compliance management in CC to corporate compliance management. Phase 2 of Case Study 1

Respondents believe the current contribution of compliance management in cloud computing to corporate compliance management is average (45%) or average (46%) in most cases while in 9% of the cases it is very high.

Following the approach taken in Phase1, the following table gathers numeric information about respondents coding Likert scales (1-5) with their corresponding values by providing their statistical descriptions. In the table Mean (M) and Standard Deviation (SD) of the different variables is provided:

Table 34. Compliance evaluation sheet. Phase 2 of Case Study 1

	M	SD
Satisfaction CC service	4.09	.539
Satisfaction compliance management in CC	4.00	.632
Contribution compliance management in CC to IT quality of service	3.73	.786
Contribution compliance management in CC to the organizational compliance management	3.64	.674

Regarding the first variable, the overall satisfaction with the CC service is quite high (4.09) and the dispersion is moderate according to the standard deviation. It is worth to note that the overall satisfaction with the compliance management aspect is quite high (4.00), but also it is important to take into account that the standard deviation is moderately high too (.632), showing a remarkable dispersion. The third variable is the contribution of compliance management to the overall IT quality of service. This aspect is quite moderate according to its mean (3.73) and also presents a high dispersion (.786). Finally, the contribution of compliance management to the overall compliance management presents the lowest score around (3.64) and the dispersion is again quite high (.674).

The second step in the analysis is the comparison of results among roles. The aim is to compare opinions to check for differences among roles. In Case Study 1, just three roles are presented, namely CIO, Manager and Group Leader. In order to know if there are statistical differences among roles, the ANOVA test has been applied. Results show there are not significant statistical differences among groups in variables studied. The following table summarizes results obtained for the variables studied:

Table 35. ANOVA results among roles. Phase 2 of Case Study 1

	ANOVA
Satisfaction CC service	F(10)=.107, p>0,05
Satisfaction compliance management in CC	F(10)=1.647, p>0,05
Contribution compliance management in CC to IT quality of service	F(10)=3.418, p>0,05
Contribution compliance management in CC to the organizational compliance management	F(10)=.278, p>0,05

However, there is a need to know if there are statistical significant differences between roles analysed in pairs. Using the Student's t-test, the author obtained the mean differences between variables group grouped in pairs. The following table presents Student T test results of the comparison between CIOs and Managers:

Table 36. Student T test results between CIO and Managers. Phase 2 of Case Study 1

	Student T test
Satisfaction CC service	t (4)=.000, p>0,05
Satisfaction compliance management in CC	t (4)=.000, p>0,05
Contribution compliance management in CC to IT quality of service	t (4)=.000, p>0,05
Contribution compliance management in CC to the organizational compliance management	t (4)=.447, p>0,05

According to data provided, there are no statistical differences between populations. The following table presents Student T test results of the comparison between CIOs and Group Leaders.

Table 37. Student T test results between CIO and Group Leaders. Phase 2 of Case Study 1

	Student T test
Satisfaction CC service	t (6)=-.378, p>0,05
Satisfaction compliance management in CC	t (6)=1.435, p>0,05
Contribution compliance management in CC to IT quality of service	t (6)=1.890, p>0,05
Contribution compliance management in CC to the organizational compliance management	t (5)=.553, p>0,05

Consistent with data provided, there are no statistical differences between populations. The following table presents Student T test results of the comparison between Managers and Group Leaders.

Table 38. Student T test results between Managers and Group Leaders. Phase 2 of Case Study 1

	Student T test
Satisfaction CC service	t (9)=.434, p>0,05
Satisfaction compliance management in CC	t (9)=-.434, p>0,05
Contribution compliance management in CC to IT quality of service	t (9)=1.600, p>0,05
Contribution compliance management in CC to the organizational compliance management	t (9)=-.531, p>0,05

Once more, according to data provided, there are no statistical differences between populations.

COMPLIANCE METRICS

One more time, the second questionnaire was circulated among CIOs or similar roles in the two companies. In the following table, main figures for the five KPIs are presented:

Table 39. Main Compliance Metrics. Phase 2 of Case Study 1

Metric	Value

Average time lag between identification of external compliance issues and resolution	45
Number of compliance issues where employees seek guidance or assistance	20
Number of reports of alleged or actual Compliance violations	61
Percentage of compliance improvement opportunities implemented	79
Frequency (in days) of compliance reviews	60

As depicted in the previous table, metrics were collected before the implementation of the framework in order to be later analysed comparing data recorded in Phase 1 and Phase 2.

7.4.2.1.2 CMMI Based Evaluation

As already mentioned above, maturity levels were assessed again twelve weeks after the framework was introduced within the organization. Here, all questions related to maturity level two were answered positively (Table 40).

Table 40. Answered Questions related to Maturity Level 2 after Framework Introduction (in German)

#	Frage	Ja	Überwiegend, mit wenigen Ausnahmen	Nein
1.	Werden Projekte/Prozesse des Bereiches auf strukturierte, reproduzierbare Art und Weise durchgeführt?	X		
2.	Werden alle Projekte/ Prozesse gemäß einer Unternehmensleitlinie geplant?		X	
3.	Werden alle Projekte und Prozesse gemäß einer Unternehmensleitlinie durchgeführt?		X	
4.	Wird zur Ausführung aller Projekte und Prozesse Fachpersonal mit angemessenen Ressourcen eingesetzt?	X		
5.	Werden relevante Stakeholder (Mitarbeiter, Kunden, Management, etc.) eingebunden?		X	
6.	Werden alle Arbeitsabläufe in den Projekten/Prozessen überwacht?		X	
7.	Werden alle Arbeitsabläufe in den Projekten/Prozessen gesteuert?	X		
8.	Werden alle Arbeitsabläufe in den Projekten/Prozessen geprüft?	X		
9.	Wird die Einhaltung der Projekt-/Prozessbeschreibungen bewertet?	X		
10.	Ist der Zustand der Arbeitsergebnisse für das Management an definierten Punkten sichtbar (zum Beispiel Meilensteine)?		X	
11.	Werden verpflichtende Inputs relevanter Stakeholder etabliert?		X	
12.	Werden verpflichtende Inputs relevanter Stakeholder bedarfsgerecht überarbeitet?	x		

13.	Werden die Arbeitsergebnisse angemessen gelenkt?		X	
14.	Erfüllen die Arbeitsergebnisse die spezifizierten Prozessbeschreibungen, Normen und Verfahren?		X	

Furthermore, questions related to maturity level three were mostly answered positively (Table 41). Specifically, three questions were answered positively, twelve were answered mostly positively, with few exceptions, and eight were answered negatively.

Table 41. Answered Questions related to Maturity Level 3 after Framework Introduction (in German)

#	Frage	Ja	Überwiegend, mit wenigen Ausnahmen	Nein
1.	Sind alle Arbeitsabläufe der Projekte/Prozesse des Bereiches gut charakterisiert und verstanden?		X	
2.	Werden die Arbeitsabläufe beschrieben in Form von Normen?			X
3.	Werden die Arbeitsabläufe beschrieben in Form von Verfahren?		X	
4.	Werden die Arbeitsabläufe beschrieben in Form von Hilfsmitteln?		X	
5.	Werden die Arbeitsabläufe beschrieben in Form von Methoden?		X	
6.	Leitet sich der Projektablauf für alle Projekte/Prozesse des Bereiches aus einem Satz von organisationsspezifischen Standardprozessen ab?			X
7.	Werden die Standardprozesse individuell auf die Bedürfnisse des Projektes/Prozesses angepasst?		X	
8.	Sind die Standardprozesse etabliert?		X	
9.	Sind die Standardprozesse kontinuierlich verbessert worden?			X
10.	Sind Richtlinien vorhanden, die die Anpassung der Standardprozesse für spezifische Projekte definieren?			X
11.	Enthalten diese Richtlinien Anweisungen zu zulässigen Anpassungen der Standardprozesse?			X
12.	Sind die Prozess-/Projektbeschreibungen streng beschrieben hinsichtlich Zweck?	X		
13.	Sind die Prozess-/Projektbeschreibungen streng beschrieben hinsichtlich Eingangsgrößen?	X		
14.	Sind die Prozess-/Projektbeschreibungen streng beschrieben hinsichtlich Eingangskriterien?		X	
15.	Sind die Prozess-/Projektbeschreibungen streng beschrieben hinsichtlich Tätigkeiten?		X	
16.	Sind die Prozess-/Projektbeschreibungen streng beschrieben hinsichtlich Rollen?		X	
17.	Sind die Prozess-/Projektbeschreibungen streng beschrieben hinsichtlich Messgrößen?			X
18.	Sind die Prozess-/Projektbeschreibungen streng beschrieben hinsichtlich Verifizierungsschritten?			X
19.	Sind die Prozess-/Projektbeschreibungen streng beschrieben hinsichtlich Ergebnissen?		X	
20.	Sind die Prozess-/Projektbeschreibungen streng beschrieben hinsichtlich Ausgangskriterien?			X
21.	Werden die Projekte/Prozesse proaktiv geführt?	X		
22.	Sind die Beziehungen zwischen einzelnen Prozesstätigkeiten und den Kenngrößen der Projekte/Prozesse und der Arbeitsergebnisse verstanden?		X	
23.	Werden Projekte/Prozesse kontinuierlich verbessert?		X	

Based on the results from Table 41 the overall achieved maturity level (ML) after the introduction of the framework can be estimated as follows (assuming that all questions are weighted equally):

$$\begin{aligned} \text{Total ML} &= \text{ML with completely positive answers} \\ &\quad + \frac{\text{number of positive answers at the higher ML}}{\text{number of all questions at the higher ML}} = 2 + \frac{15}{23} \\ &= \mathbf{2,65} \end{aligned}$$

Thus, the introduction of the framework delivered an overall increase of ML from 1 to 2.65 which represents a substantial improvement. Furthermore, this was achieved only within twelve weeks after the initial implementation of the framework. So, it can be expected that the framework would lead to further increase in maturity levels over a period of extended use and further implementation.

7.4.2.2 Case Study 2

As indicated in Phase 1, each case study provides two different sources of information. Firstly, the one gathered by means of the two previously described questionnaires and secondly, the CMMI based evaluation. Once more, these two sets are described in the following lines in the scenario drawn after the implementation of the framework:

7.4.2.2.1 Questionnaires

COMPLIANCE EVALUATION SHEET

One more time, in this phase, same respondents answered the questionnaire, so sample composition and characteristics are the same explained in Phase 1. Regarding the four specific questions labelled using a Likert scale, the distribution of responses with regards to the satisfaction on Compliance Management in CC, this is as follows:

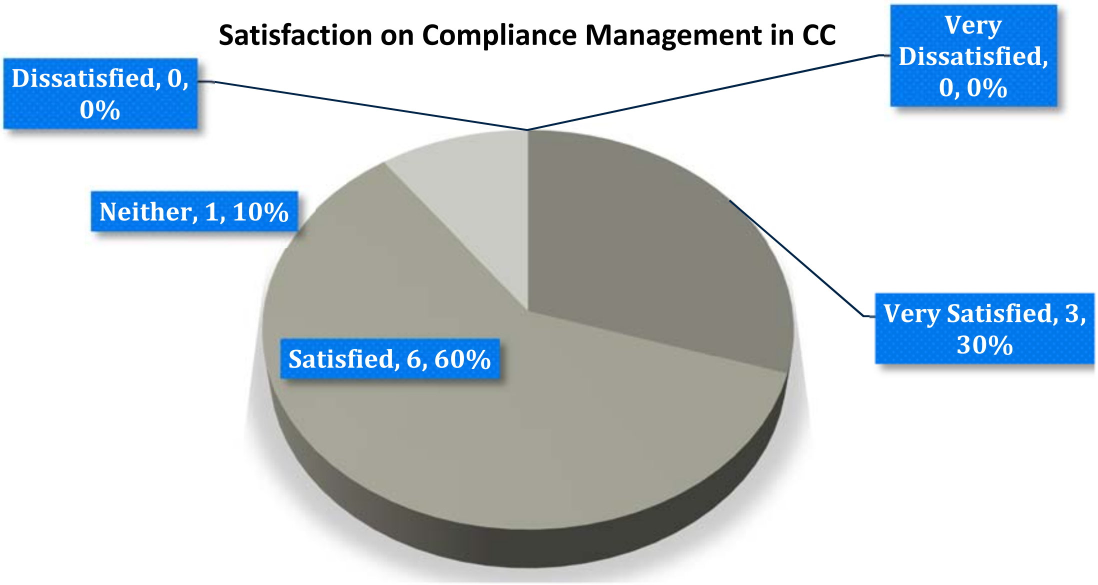


Figure 30. Satisfaction Compliance Management in CC. Phase 2 Case Study 2

As pictured in the previous figure, most of the respondents felt satisfied with compliance management (60%) or very satisfied (30%) while just 10% remain neutral on the topic. No respondents are dissatisfied after the implementation of the framework.

With regards to the Satisfaction on the CC service in the organization, distribution and answers are coded in the following figure:

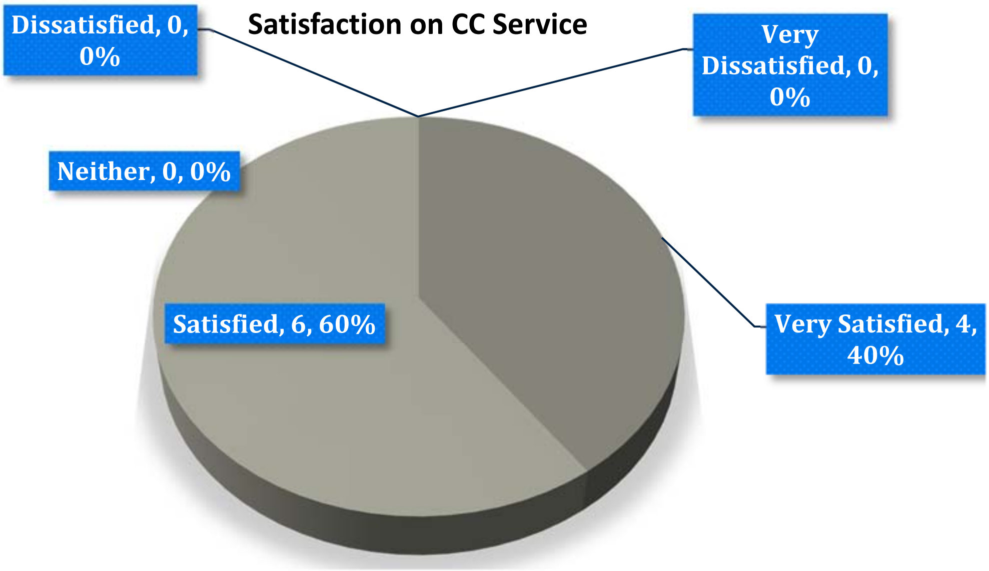


Figure 31. Satisfaction on CC Service. Phase 2 Case Study 2

As pictured in the previous figure, most of the respondents felt satisfied with CC service (60%) with it, while 2 participants very satisfied (40%). There are not negative or neutral values coded by respondents.

With regards to the contribution of compliance management in CC to IT quality of service, distribution and answers are coded in the following figure:

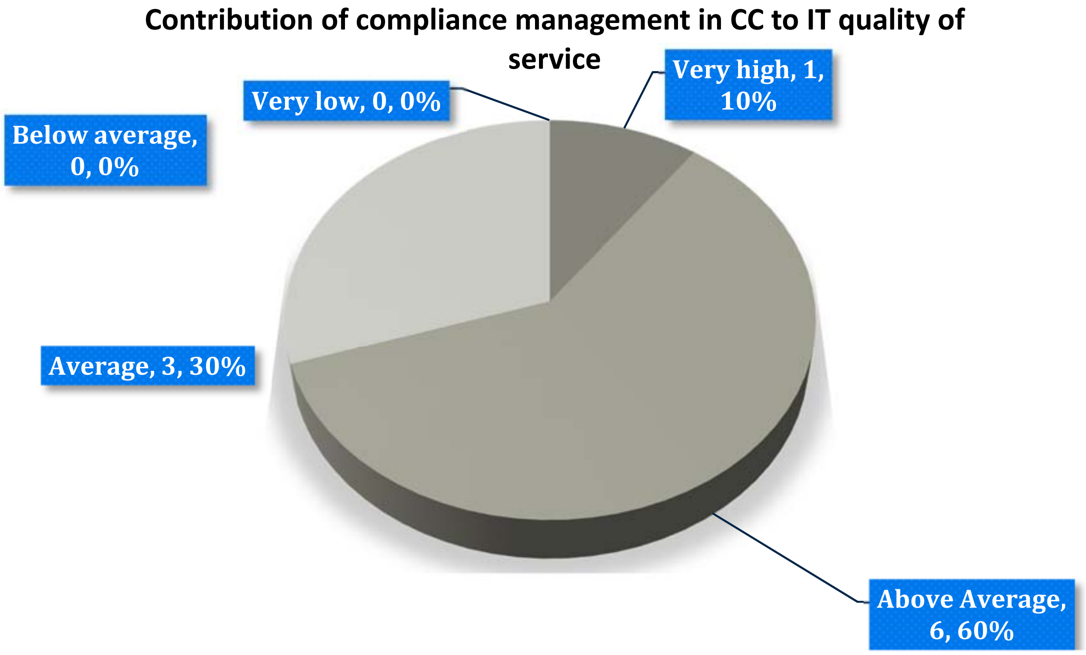


Figure 32. Contribution of compliance management in CC to IT quality of service. Phase 2 Case Study 2

Respondents believe the current contribution of compliance management in cloud computing to IT quality of service is average (30%), while in 60% of the cases it is above average and 10% of the cases is very high.

The last piece of information taken from the questionnaire is the opinion on the contribution of compliance management in the field of CC to the corporate compliance management. This is presented in the following figure:

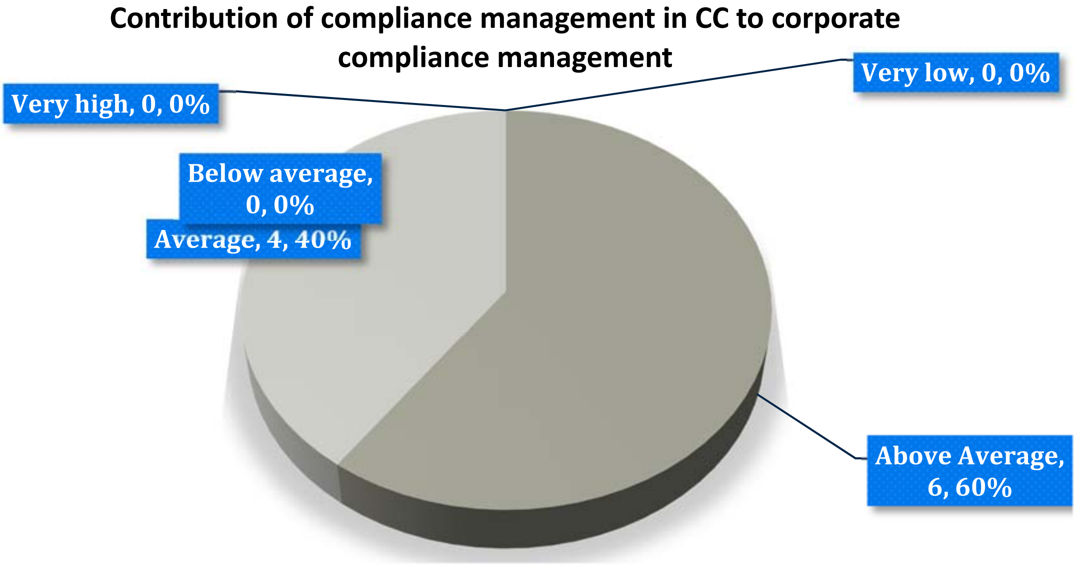


Figure 33. Contribution of compliance management in CC to corporate compliance management. Phase 2 Case Study 2

Respondents believe the current contribution of compliance management in cloud computing to corporate compliance management is average (40%) or above average (60%).

Following the approach adopted for Case study 1 and Phase 1, the following table gathers numeric information about respondents coding Likert scales (1-5) with their corresponding values by providing their statistical descriptions. In the table Mean (M) and Standard Deviation (SD) of the different variables is provided:

Table 42. Compliance evaluation sheet. Phase 2 of Case Study 2

	M	SD
Satisfaction CC service	4.40	.516
Satisfaction compliance management in CC	4.20	.632
Contribution compliance management in CC to IT quality of service	3.80	.632
Contribution compliance management in CC to the organizational compliance management	3.60	.516

Regarding the first variable, the overall satisfaction with the CC service is, again, quite high (4.40) and the dispersion is just moderate, according to the standard deviation (.516). It is worth to note that the overall satisfaction with the compliance management aspect is quite high (4.20), but also it is important to take into account that the standard deviation is, again, the highest among the variables (.632), showing a remarkable dispersion. The third variable is the contribution of compliance management to the overall IT quality of service. This aspect is more moderated according to its mean (3.80) and also presents a moderate relatively high (.632). Finally, the contribution of compliance management to the overall compliance management presents same figures lowest figures (3.60) and the dispersion is also moderate(.516).

The second step in the analysis is the comparison of results among roles. The aim is to compare opinions to check for differences among roles. In Case Study 2, just three roles are presented namely CIO (In this category we add also Vice-president to be consistent with Case 1), Manager and Group Leader. In order to know if there are statistical differences among roles, the ANOVA test has been applied. Results show there are no significant statistical differences among groups in the four variables studied. The following table summarizes results obtained for the variables studied:

Table 43. ANOVA results among roles. Phase 2 of Case Study 2

	ANOVA
Satisfaction CC service	F(9)=2.800, p>0,05
Satisfaction compliance management in CC	F(9)=.280, p>0,05
Contribution compliance management in CC to IT quality of service	F(9)=1.900, p>0,05
Contribution compliance management in CC to the organizational compliance management	F(9)=.700, p>0,05

However, there is a need to know if there are statistical significant differences between roles analysed in pairs. Using the Student's t-test, we obtained the mean differences between variables group in pairs. The following table presents Student T test results of the comparison between CIOs and Managers.

Table 44. Student T test results between CIOs and Managers. Phase 2 of Case Study 2

	Student T test
Satisfaction CC service	t (3)=1.000, p>0,05
Satisfaction compliance management in CC	t (3)=1.000, p>0,05
Contribution compliance management in CC to IT quality of service	t (3)=1.414, p>0,05
Contribution compliance management in CC to the organizational compliance management	t (3)=1.000, p>0,05

According to data provided, there are no statistical differences between populations. The following table presents Student T test results of the comparison between CIOs and Group Leaders.

Table 45. Student T test results between CIOs and Group Leaders. Phase 2 of Case Study 2

	Student T test
Satisfaction CC service	t (7)=.548, p>0,05
Satisfaction compliance management in CC	**t (7)=2.739, p<0,05**
Contribution compliance management in CC to IT quality of service	t (7)=1.846, p>0,05
Contribution compliance management in CC to the organizational compliance management	t (7)=1.225, p>0,05

The only significant statistical difference found is the second variable in which CIOs and Groups leaders present different opinions on the satisfaction of Compliance Management in CC. This is due to the high satisfaction perceived by top managers compared to the one expressed by Group Leaders. The following table presents Student T test results of the comparison between Managers and Group Leaders.

Table 46. Student T test results between Managers and Group Leaders. Phase 2 of Case Study 2

	Student T test
Satisfaction CC service	t (7)=-.297, p>0,05
Satisfaction compliance management in CC	t (7)=-.866, p>0,05
Contribution compliance management in CC to IT quality of service	t (7)=-.369, p>0,05
Contribution compliance management in CC to the organizational compliance management	t (7)=-.000, p>0,05

Once more, according to data provided, there are no statistical differences between populations.

COMPLIANCE METRICS

One more time, the second questionnaire was circulated among CIOs or similar roles in the two companies. In the following table, main figures for the five KPIs are presented:

Table 47. Main Compliance Metrics. Phase 2 Case Study 2

Metric	Value
Average time lag between identification of external compliance issues and resolution	35
Number of compliance issues where employees seek guidance or assistance	11
Number of reports of alleged or actual Compliance violations	58
Percentage of compliance improvement opportunities implemented	78
Frequency (in days) of compliance reviews	30

One more time, metrics were collected before the implementation of the framework in order to be later analysed comparing data recorded in Phase 1 and Phase 2.

7.4.2.2.2 CMMI Based Evaluation

As already mentioned above, maturity levels were assessed again twelve weeks after the framework was introduced within the organization (Table 48). The layout of the table corresponds to the requirements that were elicited together with evaluation partner 2 during the customization phase of the framework and again reflect the technology-oriented paradigm of this organization.

Table 48. Questions related to different Maturity Levels (ML, column 1) and Answers (yes/no) per Areas after Framework Introduction at Partner 2 / Case Study 2

Level (ML)	Question No.	Question	network	applications	authorization concept	anti-virus	cryptography	patch-/change-	archiving and backup	infrastructure	logging
2	1	Is the process planned and executed in accordance with policy?	no	no	no	no	no	no	no	no	no
2	2	Is there a responsible unit / work group for – defining service strategy? – creating work plans? – monitoring and controlling work?	no	yes	yes	yes	yes	yes	yes	yes	yes

2	3	Regarding process execution, do the following apply? – adequate resources are available? – responsibilities are assigned? – people are trained on the process? – work products are under appropriate configuration management levels?	no	no	no	no	no	no	no	no	no
2	4	Are customer and contractual requirements developed and managed?	no	no	no	no	no	no	no	no	no
2	5	Are relevant stakeholders identified and involved?	yes	yes	yes	yes	yes	yes	yes	yes	yes
2	6	Are the following managed: – work groups? – work activities? – process? – work product? – service?	no	no	no	no	no	no	no	no	no
2	7	Can process performance be measured and analyzed?	no	no	no	no	no	no	no	no	no
2	8	Is process adherence periodically – evaluated? – reviewed? – shared with senior management?	yes	yes	yes	yes	yes	yes	yes	yes	yes
3	1	Is the process described in – standards, – procedures, – tools, and – methods?	yes	yes	yes	yes	yes	yes	yes	yes	yes
3	2	Is the process tailored from a standard process (set)?	no	yes	yes	yes	no	no	yes	no	no
3	3	Is the process tailoring done according to tailoring guidelines?	yes	yes	yes	yes	yes	yes	yes	yes	yes

3	4	Does this standard process embed tenets of – project and work management? – best practices (e. g. service continuity, incident resolution and prevention)	yes	yes	yes	yes	yes	yes	yes	yes	yes
3	5	Are work product's requirements verified?	yes	yes	yes	yes	yes	yes	yes	yes	yes
3	6	Are services validated to ensure customer and end-user requirements are met?	yes	yes	yes	yes	yes	yes	yes	yes	yes
3	7	Does the process definition clearly state – purpose? – inputs? – entry criteria? – activities? – roles? – measures? – verification steps? – outputs? – exit criteria?	no	no	no	no	no	no	no	no	no
3	8	Is the defined process rigorously performed according to detailed process descriptions?	no	no	no	no	no	no	no	no	no
3	9	Is there an understanding of interrelations between process activities and detailed measures of the process, its work products and its services?	no	no	no	no	no	no	no	no	no
4	1	Are quantitative objectives for quality and process performance established?	no	no	no	no	no	no	no	no	no
4	2	Are quantitative objectives established, based on the needs of – the customer? – the end user? – organization?	no	no	no	no	no	no	no	no	no

		– process implementers?									
4	3	Is quality and process performance – understood in statistical terms? – managed throughout the life of the process?	no	no	no	no	no	no	no	no	no
4	4	Is process performance predictable, based on statistical data and fine-grained process data?	no	no	no	no	no	no	no	no	no
4	5	Can process performance baselines and models be used to help set the process' quality and performance?	no	no	no	no	no	no	no	no	no
4	6	Are there specific measures of process performance collected and statistically analysed for specific subprocesses?	no	no	no	no	no	no	no	no	no
4	7	On a subprocess level, are statistical and other quantitative techniques used for those with the highest impact on value for business?	no	no	no	no	no	no	no	no	no
5	1	Is the process continually improved, based on a quantitative understanding of its objectives and performance needs?	no	no	no	no	no	no	no	no	no
5	2	Is a quantitative approach used to understand the variation in and the causes of process outcomes?	no	no	no	no	no	no	no	no	no

5	3	Is process performance continually improved through incremental and innovative process and technological improvement	no	no	no	no	no	no	no	no	no
5	4	Quality and performance objectives are – established – continually revised – used as criteria in managing process improvement	no	no	no	no	no	no	no	no	no
5	5	Are the effects of deployed process improvements measured (through statistical or other quantitative techniques)?	no	no	no	no	no	no	no	no	no
5	6	Are those results compared against quality and process performance objectives?	no	no	no	no	no	no	no	no	no
5	7	Are the defined process, its corresponding standard process and supporting technologies targets of measurable improvement activities?	no	no	no	no	no	no	no	no	no
5	8	Is there a focus on understanding and controlling performance on a subprocess level?	no	no	no	no	no	no	no	no	no
5	9	Are those results used to manage projects?	no	no	no	no	no	no	no	no	no
5	10	Are relevant information regarding process performance aggregated to drive organizational process improvement?	no	no	no	no	no	no	no	no	no
			1	1	1	1	1	1	1	1	1

The answers in Table 48 show a high degree of variance for the different areas. Still, results show that an increase of maturity up to level two cannot be anticipated for any specific area, even in the presence of some positive answers referring to level three. There are simply too many negative answers to questions associated with level two that prevent this.

Assuming again that all questions are weighted equally, the estimation of the overall achieved maturity level (ML) per technological area was done by applying the same formula. Results are aggregated in Table 49. A visualization of results is shown in Figure 34.

Table 49. Maturity Levels per Areas before (Column 2) and after (Column 3) Framework Introduction at Partner 2 / Case Study 2

Area	Maturity Level (ML) before	Maturity Level (ML) after
network	1	1,25
applications	1	1,375
authorization concept	1	1,375
anti-virus	1	1,375
cryptography	1	1,375
patch-/change-management	1	1,375
archiving and backup	1	1,375
infrastructure	1	1,375
logging	1	1,375

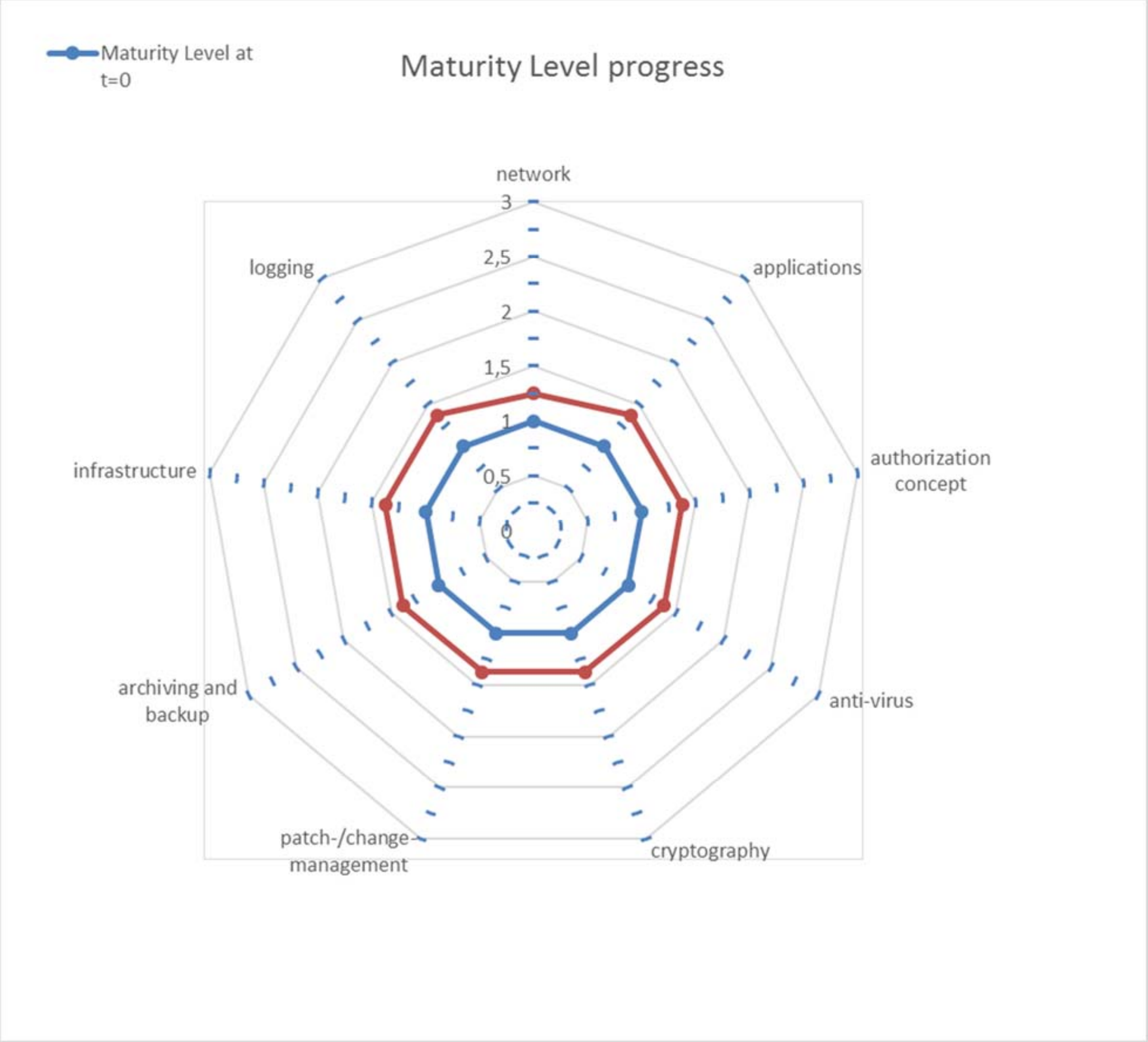


Figure 34. A Visualization of Improvement in Maturity Levels before (blue) and after (red) Framework introduction at Evaluation Partner 2 / Case Study 2

Thus, the introduction of the framework delivered an overall increase of ML from 1 to 1.3-1.5 which represents an improvement that is more modest compared to the improvement with evaluation partner 1. Nevertheless, this improvement was achieved again within twelve weeks after the initial implementation of the framework. So, it can be expected that the framework would lead to further increase in maturity levels over a period of extended use and further implementation when applied in technology-oriented organizations such as IT service providers (evaluation partner 2). The pace of this improvement appears to be slower than the pace of improvement when implemented in organizations resembling evaluation partner 1.

7.4.2.3 Overall comparison

In the following section the analysis performed to compare results obtained in both case studies are depicted, particularizing the analysis in the two instruments circulated to obtain data in Phase 2.

7.4.2.3.1 Compliance Evaluation Sheet

Following the approach adopted earlier, we will start the analysis presenting descriptive statistics of previous phases. In the table, Mean (M) and Standard Deviation (SD) of the different variables are provided:

Table 50. Descriptive statistics on compliance evaluation sheet. Phase 2, overall comparison

	CASE 1		CASE 2	
	M	SD	M	SD
Satisfaction CC service	4.09	.539	4.40	.516
Satisfaction compliance management in CC	4.00	.632	4.20	.632
Contribution compliance management in CC to IT quality of service	3.73	.786	3.80	.632
Contribution compliance management in CC to the organizational compliance management	3.64	.674	3.60	.516

In general, it is worth to note that means and standard deviations are, in both cases, comparable. However, in most cases figures in means are higher in Case 2 compared to Case 1 (in all variables but contribution compliance management in CC to the organizational compliance management), although the differences are slender. Standard deviations are also analogous in all variables although they are lower in Case 2.

The second step in the analysis is the comparison of results between cases. Using the Student's t-test, we obtained the mean differences between variables obtained in both case studies. The following table presents Student T test results of the comparison between case studies 1 and 2 in Phase 2 for the four variables.

Table 51. Student T test results between case studies. Phase 2, overall comparison

	Student T test
Satisfaction CC service	t (20)=-1.338, p>0,05
Satisfaction compliance management in CC	t (20)=-724, p>0,05

Contribution compliance management in CC to IT quality of service	t (20)=-232, p>0,05
Contribution compliance management in CC to the organizational compliance management	t (20)=-.138, p>0,05

According to data provided, there are no statistical differences between case studies for this Phase 2. This means that data is comparable between cases.

7.4.2.3.2 Compliance Metrics Questionnaire

In the following table the two sets of data are presented with regards to the compliance metrics questionnaire:

Table 52. Compliance Metrics, Phase 2, overall comparison

Metric	Case 1	Case 2
Average time lag between identification of external compliance issues and resolution	45	35
Number of compliance issues where employees seek guidance or assistance	20	11
Number of reports of alleged or actual Compliance violations	61	58
Percentage of compliance improvement opportunities implemented	79	78
Frequency (in days) of compliance reviews	60	30

Again, data is quite comparable given the different backgrounds of the two organizations. Thus, there are metrics quite comparable (Average time lag between identification of external compliance issues and resolution, Number of reports of alleged or actual Compliance violations and Percentage of compliance improvement opportunities implemented) while the last metric, that depends on the current compliance management process and not the results of it, Frequency (in days) of compliance reviews, is different. The second metric with dissimilar values is Number of compliance issues where employees seek guidance or assistance. The explanation of the difference can be found in the activity of the company. The first one is not devoted to IT, while the second is an IT company. The competence of employees in IT topics could be the cause of this disparity. However and in general, both organizations present similar data and are comparable also in Phase 2.

7.4.3 Phase 3

In what follows, details on the comparison of the data collected for both case studies are presented.

7.4.3.1 Case Study 1

In the following section the analysis performed to compare results obtained in Phases 1 and 2 is presented, particularizing the analysis in the two instruments circulated to obtain data for Case Study 1.

7.4.3.1.1 Compliance Evaluation Sheet

Following the approach adopted earlier, in this Phase 3 we will start the analysis presenting descriptive statistics of previous phases. In the table, Mean (M) and Standard Deviation (SD) of the different variables are provided:

Table 53. Descriptive statistics on compliance evaluation sheet. Phase 3 Case Study 1

	PHASE 1		PHASE 2	
	M	SD	M	SD
Satisfaction CC service	3.91	.539	4.09	.539
Satisfaction compliance management in CC	3.36	.809	4.00	.632
Contribution compliance management in CC to IT quality of service	3.09	.701	3.73	.786
Contribution compliance management in CC to the organizational compliance management	2.82	.405	3.64	.674

In general, it is important to note that means are, in all cases, higher in Phase 2 than in Phase 1, while standard deviations vary. In the case of the first variable it remains stable, while is lower for the satisfaction with the compliance management in CC. This means that respondents have less dispersion in their opinion gathering a higher consensus. Moreover, the consensus is reached on a higher satisfaction. However, regarding variables three and four, dispersion is higher in Phase 2 than in Phase 1.

The second step in the analysis is the comparison of results between Phases. Using the Student's t-test, we obtained the mean differences between variables obtained in Phases 1 and 2. The following table presents Student T test results of the comparison between Phase 1 and Phase 2 on the four variables.

Table 54. Student T test results between Phases. Case Study 1

	Student T test
Satisfaction CC service	t (10)=-.791, p>0,05
Satisfaction compliance management in CC	t (10)=-2.055, p>0,05
Contribution compliance management in CC to IT quality of service	t (10)=-2.004, p>0,05
Contribution compliance management in CC to the organizational compliance management	**t (10)=-3.451, p<0,05**

Consistent with data provided, there are no statistical differences between Phases in the first three variables, while there is statistically significant difference between them in the contribution of compliance management in CC to the overall compliance management.

7.4.3.1.2 Compliance Metrics Questionnaire

In the following table the two sets of data are presented with regards to the compliance metrics questionnaire:

Table 55. Compliance Metrics, Comparison of Phases. Case Study 1

Metric	Phase 1	Phase 2
Average time lag between identification of external compliance issues and resolution	48	45
Number of compliance issues where employees seek guidance or assistance	19	20
Number of reports of alleged or actual Compliance violations	89	60
Percentage of compliance improvement opportunities implemented	73	79
Frequency (in days) of compliance reviews	60	60

Specifics insights on the differences are as follows:

1. Regarding the average time lag between identification of external compliance issues and resolution, Phase 2 shows a slight difference (6.25%) in the resolution of compliance issues after the implementation of the framework. The difference is very limited, however, we can see it as a good sign favouring the adoption of the framework.
2. With regards to the number of compliance issues where employees seek guidance or assistance, Phase 2 shows an increment (5.26%) in the issues

identified in which employees seek for assistance. Again, differences are very slight, however, it is worth to note that the framework can be seen as a way to guide employees towards a process to guide them to the correct management of issues, including guidance among its steps.

3. Concerning the number of reports of alleged or actual Compliance violations figures decreased from 89 to 60 (32.59%). Although these figures are very encouraging, the author wants to emphasize that sample size is relatively small and the generalization of results is threatened by the impossibility of isolating the external factors from the variables. However, it is also important to consider that the improvement is aligned with the rest of the metrics presented.
4. Regarding the percentage of compliance improvement opportunities implemented, it is, again, slightly improved (8.22%). This is, again, a sign of the validity of the framework for the effective and efficient management of compliance issues.
5. The last aspect regarding frequency (in days) of compliance reviews remains stable. In this case, organization presented in Phase 1 a Compliance management process in which reviews were part of the process. This process remain unchanged in Phase 2.

7.4.3.2 Case Study 2

In the following section the analysis performed to compare results obtained in Phases 1 and 2 is depicted, particularizing the analysis in the two instruments circulated to obtain data for Case Study 2.

7.4.3.2.1 Compliance Evaluation Sheet

Following the approach adopted earlier, in this Phase 3 we will start the analysis presenting descriptive statistics of previous phases. In the table, Mean (M) and Standard Deviation (SD) of the different variables are provided:

Table 56. Descriptive statistics on compliance evaluation sheet. Phase 3 Case Study 2

	PHASE 1		PHASE 2	
	M	SD	M	SD
Satisfaction CC service	4.00	.667	4.40	.516
Satisfaction compliance management in CC	3.70	.823	4.20	.632
Contribution compliance management in CC to IT quality of service	3.10	.568	3.80	.632
Contribution compliance management in CC to the	3.10	.568	3.60	.516

organizational compliance management				

In general, it is important to note that, one more time, means are, in all cases, higher in Phase 2 than in Phase 1, while standard deviations vary. In the case of the first variable it is lower in Phase 2. Dispersion is lower also in variable two and variable four. This means that respondents have less dispersion in their opinion gathering a higher consensus. Moreover, the consensus is reached on a higher satisfaction. However, regarding variables three, dispersion is higher in Phase 2 than in Phase 1.

The second step in the analysis is the comparison of results between Phases. Using the Student's t-test, we obtained the mean differences between variables obtained in Phases 1 and 2. The following table presents Student T test results of the comparison between Phase 1 and Phase 2 on the four variables.

Table 57. Student T test results between Phases. Case Study 2

	Student T test
Satisfaction CC service	t (9)=-1.500, p>0,05
Satisfaction compliance management in CC	t (9)=-1.523, p>0,05
Contribution compliance management in CC to IT quality of service	**t (9)=-2.605, p<0,05**
Contribution compliance management in CC to the organizational compliance management	t (9)=-2.060, p>0,05

According to data provided, there are no statistical differences between Phases in the first three variables, while there is statistical significant difference between them in the contribution of compliance management in CC to the IT quality of service.

7.4.3.2.2 Compliance Metrics Questionnaire

In the following table the two sets of data are presented with regards to the compliance metrics questionnaire:

Table 58. Compliance Metrics, Comparison of Phases. Case Study 2

Metric	**Phase 1**	**Phase 2**
Average time lag between identification of external compliance issues and resolution	36	35
Number of compliance issues where employees seek guidance or assistance	12	11

Number of reports of alleged or actual Compliance violations	76	58
Percentage of compliance improvement opportunities implemented	75	78
Frequency (in days) of compliance reviews	30	30

Specifics insights on the differences are as follows:

1. Regarding the average time lag between identification of external compliance issues and resolution, Phase 2 shows a slight difference (2.18%) in the resolution of compliance issues after the implementation of the framework. The difference is, once again, very limited, however, we can see it as a good sign favouring the adoption of the framework.
2. With regard to the number of compliance issues where employees seek guidance or assistance, Phase 2 shows a decrement (9.10%) in the issues identified in which employees seek for assistance. Again, differences are very slight, however, and confronting with previous explanation, the reason behind this can be rooted in the more detailed process implemented with the framework
3. Concerning the number of reports of alleged or actual Compliance violations figures decreased from 76 to 58 (23.78%). While these figures are very encouraging, we want to emphasize that sample is, again, relatively small and the generalization of results is threatened by the impossibility of isolating the external factors from the variables. However, it is also important to consider that the improvement is aligned with the rest of the metrics presented.
4. Regarding the percentage of compliance improvement opportunities implemented, it is, again, slightly improved (4%). This is, again, a sign of the validity of the framework for the effective and efficient management of compliance issues.
5. The last aspect regarding frequency (in days) of compliance reviews remains stable. Like in the previous case, a compliance management process was already implemented in the organization. This process remained unchanged in Phase 2.

7.4.3.3 Overall comparison

The final step in the analysis of cases will be the comparison of the whole sample mixing data from both case studies in order to generalize findings previously detected. Again, this comparison will be performed with regard to the two sources of information employed in the study.

7.4.3.3.1 Compliance Evaluation Sheet

Following the approach adopted earlier, we will start the analysis presenting descriptive statistics of previous phases. In the table, Mean (M) and Standard Deviation (SD) of the different variables are provided:

Table 59. Descriptive statistics on compliance evaluation sheet. Phase 3, overall comparison

	PHASE 1		PHASE 2	
	M	SD	M	SD
Satisfaction CC service	3.95	.590	4.24	.539
Satisfaction compliance management in CC	3.52	.814	4.10	.625
Contribution compliance management in CC to IT quality of service	3.10	.625	3.76	.700
Contribution compliance management in CC to the organizational compliance management	2.95	.498	3.62	.590

In general, it is worth to note that means and standard deviations are, in both cases, comparable but always higher in Phase 2. Standard deviations are also analogous and vary with variables.

The second step in the analysis is the comparison of results between phases in an integrated way. Using the Student's t-test, we obtained the mean differences between variables obtained in both phases. The following table presents Student T test results of the comparison between aggregated data obtained in Phase 1 and 2 for the four variables.

Table 60. Student T test results between case studies. Phase 3, overall comparison

	Student T test
Satisfaction CC service	t (20)=-1.639, p>0,05
Satisfaction compliance management in CC	**t (20)=-2.553, p<0,05**
Contribution compliance management in CC to IT quality of service	**t (20)=-3.255, p<0,05**
Contribution compliance management in CC to the organizational compliance management	**t (20)=-3.960, p<0,05**

Consistent with data provided, there are three variables with statistical differences between phases: Satisfaction compliance management in CC, Contribution compliance management in CC to IT quality of service, Contribution compliance management in CC to the organizational compliance management. So, this means that in these cases, the framework is improving given KPIs affected.

7.4.3.3.2 Compliance Metrics Questionnaire

In the following table the two sets of data are presented with regards to the compliance metrics questionnaire calculating the average of both case studies:

Table 61. Compliance Metrics, Phase 3, overall comparison

Metric	Phase 1	Phase 2
Average time lag between identification of external compliance issues and resolution	42	40
Number of compliance issues where employees seek guidance or assistance	15.5	15.5
Number of reports of alleged or actual Compliance violations	82	59.5
Percentage of compliance improvement opportunities implemented	74.5	78.5
Frequency (in days) of compliance reviews	45	45

Again, data is quite comparable between phases. Thus, there are metrics quite comparable (Average time lag between identification of external compliance issues and resolution, Number of compliance issues where employees seek guidance or assistance, Percentage of compliance improvement opportunities implemented and Frequency of compliance reviews) while the last metric, Number of reports of alleged or actual Compliance violations, is very different. There is a significant decrease in the number of reports with compliance violations, a positive symptom for the framework. Other less remarkable improvements are slightly better figures in resolution times and percentage of compliance improvement opportunities implemented.

7.5 Revisiting the research questions and hypotheses

In this section, research questions and hypotheses are discussed in the light of the two case studies. According to results, after the development of this doctoral thesis, it exists an appropriate compliance framework to support organizations in compliance issues in CC environments.

Regarding the general hypothesis, and taking into account that there is a framework that is able to fulfil compliance needs in CC settings, this framework has been adapted for and introduced within two different organizations where it has improved previous compliance processes according to several metrics and the satisfaction of the compliance management processes. It also enhanced the perception of the contribution of compliance management in CC to IT quality of service and the contribution of compliance management in CC to the organizational compliance management. Finally, and in a lesser extent, there is an improvement in the satisfaction with CC service.

7.6 Discussion of Results

The evaluation of the framework was conducted following important feedback from committee members during pre-dissertation. This resulted in a transformation of the original evaluation approach that was focused more to the input areas to a more holistic approach that assesses the impact of the framework as a whole. However, the original idea to test the repercussion of the framework also took into account specific KPIs. Nevertheless, this transformation required careful selection of evaluation partners in order to provide reliable and generally applicable results as already specified in previously in this chapter. In order to follow previous approach on the evaluation, discussion will be divided into two main sections depicted in what follows, the first devoted to discuss results on questionnaires and the second devoted to debate results on the CMMI based evaluation.

7.6.1 Questionnaire Based Evaluation

In order to review main results and discuss them comparing our findings with relevant literature, we will divide discussion among the three phases in the study.

7.6.1.1 Phase 1

Phase 1 consists in collecting information on compliance management in CC environments before the implementation of the framework in both case studies.

The first finding worth to note is the different perspectives found in the contribution of compliance management in CC to IT quality of service from the viewpoint of CIOs and Group Leaders detected in Phase 1 of Case Study 1. It was revealed by a Student T test presenting significant values t (6) = 2.646, p<0,05. Compliance management has been identified as one of the aspects to measure IT service quality (Bhamidipaty et al., 2009; Lepmets, Cater-Steel, Gacenga, & Ras, 2012; Singh & Sidhu, 2017). Taking into account that IT service quality as the perceived performance of the level of IT customer service provided to an organization (Lowry & Wilson, 2016), IT service quality depends somehow on the subject, organization and moment in time. So, it is not surprising finding different opinions on the subject. Nevertheless, previous works by these authors found there is no significant difference in perceptions between managers/executives and other IT staff (Lowry & Wilson, 2016). However, in our case, this is not true. Maybe the reason behind this can be found in other definition of service quality "a client perception based on a comparison between actual service performance and expectations of service" (Grönroos, 1984). We can argue that the expectations of the service could be different between the two groups and Group Leaders have higher expectations than CIOs. As a result of this, the perceptions of CIOs are statistically significantly higher as reported in this study.

The second interesting finding in this phase is the significant differences found in the Satisfaction of CC service among roles, detected by the ANOVA test performed. F(9)=7.000, p<0,05 in Case Study 2. This is mainly backed up by the differences found in the opinions of CIOs and Group Leaders detected in the Student T test results t (7)=3.464, p<0,05 performed between groups. The topic of outsourced IT services has been tackled vastly in scientific literature from different perspectives e.g. (El-Gazzar, Hustad, & Olsen, 2016; Schneider & Sunyaev, 2015; Walterbusch, Martens, & Teuteberg, 2015). In works like (McNaughton et al., 2010), the problem of the integration of IT users perspective is depicted. These authors suggest the inclusion of opinions of the individuals who need the systems, technology, equipment, products and services of the IT department on a daily basis to support business processes. However, and again the problem in this matter is more connected with the previous finding in which managers´ perceptions are normally higher than other workers perceptions on the service provided or the product developed.

7.6.1.2 Phase 2

Phase 2 consists in collecting information on compliance management in CC environments after the implementation of the framework in both case studies.

In Phase 2, the only aspect worth to mention is connected with the second finding in the previous phase regarding the perception of Satisfaction of CC service. Although this time we cannot find differences detected in the ANOVA test, there are differences found in the opinions of CIOs and Group Leaders detected in the Student T test results t (7)=2.739, p<0,05 performed between groups. Once again, the problem in this matter is more connected with the previous finding in which managers´ perceptions are normally higher than other workers perceptions on the service provided or the product developed.

7.6.1.3 Phase 3

Phase 3 consists in the comparison of the two sets of data collected in previous phases. We will focus the analysis in the overall comparison performed, given the comparable results obtained in both cases.

The first set of findings are coming from the Compliance Evaluation Sheet. As pointed out before, means of the satisfaction and contribution after the use are higher in Phase 2, meaning the framework is, in general, positive in the aspects measured. This is, maybe the most important finding of all, given that this one of the objectives of this work. However, it is also important to note that, regarding the variable of Satisfaction on compliance management in CC, maybe the most important variable in the questionnaire, apart from a better score (reaching 4.10 from the previous 3.52), standard deviation is also lower (.625 compared to .814). This circumstance is also present in Satisfaction with CC service but presenting less differences in the standard deviation scores.

The increase of satisfaction and contribution of the framework is backed up by the fact that there are significant differences in three of the four variables analysed comparing the pre and the 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).

However, it is also important to note that the adoption of the framework is not affecting the satisfaction of CC service in a significant way. While it is true that mean has enhanced and standard deviation is slightly lower, it is not statistical significant according to the Student T test results (t (20) =-1.639, p>0,05).

7.6.2 CMMI Based Evaluation

The evaluation results with evaluation partner 1 demonstrated the benefits that the framework can bring to a complex organization from the perspective of IT service users with complex regulatory requirements. Here, the focus of the framework and its benefits lie clearly at the interface between the internal IT service delivery and the different business units. This insight was present already during the customization of the framework and it was later confirmed during the actual evaluation phase. The substantial increase in maturity levels (approx. 1.5 levels) in the relatively short period of time (twelve weeks) clearly shows that the framework can reap fast and sustained benefits in organizations that have complex internal processes that involve the IT service delivery unit and various business units. Furthermore, the framework is able to improve transparency of compliance both at the supply and demand side of IT services within the organization.

The evaluation results with evaluation partner 2 aimed to present a complimentary scenario to the one with evaluation partner 1. This was the scenario of the IT service provider who wants to make compliance of cloud services one of his competitive advantages. From the perspective of this organization the complexity lies no so much within the interaction between the organization and its customers, but is more focused in the different technological subject areas. Specifically, while there is a predominant technological paradigm applied within the organization, the compliance-oriented view was underrepresented and – more importantly – was not aligned with the technological side. Here again, the framework led to an increase in overall maturity levels (approx. 0.5). Thus, this second evaluation can also be considered successful, even though the effects of the introduction of the framework were not so pronounced as in the case of evaluation partner 1.

Overall, the evaluation demonstrated several important aspects related to the framework. First, it showed the general applicability and practicability of the framework. Both organizations were able to understand its underlying paradigms and to map its general promise to tangible success factors. Second, the IT compliance experts in the two organizations were able to identify themselves with the main assumptions and paradigms of the framework which shows that the framework is well aligned with state-of-the-art approaches in IT compliance. Third, the successful customization of the framework for the two very different evaluation partners demonstrated that it can be applied to a wide range of organizations. Fourth, the implementation of the framework proved to be straightforward and was completed within 2-3 months in both organizations. This showed that the negative effects during the implementation on the running operations of the organizations can be successfully minimized. Finally, the ability to show clear and documented improvements within the short timeframe of twelve weeks is a further demonstration that the framework represents a powerful and adequate approach for handling change management of cloud environments in a compliant way.

8 Conclusion and Outlook

This chapter aims to assess the accomplishment of the postulated objectives, to list the main contributions of the thesis and the benefits that the proposed framework can provide to organisations. Furthermore, it discusses the potentials for future applications and further development of the framework and also provides an outlook on future research activities in the area.

Cloud systems still face some obstacles to their adoption (Colomo-Palacios, Fernandes, Sabbagh, & de Amescua Seco, 2012). Specific doubts remain that externally controlled cloud services can be adequately protected, and industry-specific offerings are being assessed to ensure security and privacy (Liu, 2012). Health systems are crucial when considering technological developments, and the importance of the cloud for the health sector has been underlined by previous studies in countries such as China (Kshetri, 2013). In the regulation field, literature has analysed cloud services in several environments including general studies on EU data privacy regulations (Kshetri & Murugesan, 2013), general records management (Rodrigues, de la Torre, Fernandez, & Lopez-Coronado, 2013), and US federal electronic health record regulations (Schweitzer, 2012) along with studies devoted to analysing trans-border health data in cloud settings (Seddon & Currie, 2013).

In this context, the proposed thesis builds on all these existing approaches and contributes a valuable differentiation of input areas that need to be considered in order to assure compliance in the change management with respect to cloud computing offerings. Furthermore, the proposed detailed approaches for considering inputs that are tailored to the different domain areas of the inputs allow a more complete and thorough assessment and thus ensure a higher level of compliance.

This chapter aims to assess the accomplishment of the postulated objectives, to list the main contributions of the thesis and the benefits that the proposed framework can provide to organisations. Furthermore, it discusses the potentials for future applications and further development of the framework and also provides an outlook on future research activities in the area.

8.1 Accomplishment of Objectives

The presented thesis introduced a Compliance Framework for Change Management in Cloud Environments (CFC MCC) that was validated by experts and evaluated in real-world organisational settings. As part of this work the following research objectives have been accomplished:

Objective 1. Investigate and gather existing models, constructs and approaches within the industry and the research community related to the aims of this work.

This objective was accomplished by analysing and specifying the relevant subject areas and conducting a rigorous analysis of existing literature in these areas.

Objective 2. Collect, unify and improve existing approaches if any, and propose new techniques and standards if required to solve the described problem.

Existing approaches were solicited, improved and then integrated together with newly developed techniques and methods into the proposed framework.

Objective 3. Devise and design an approach, based on study previously performed, and with the capabilities for meeting the research challenges pointed out in this document.

An approach that follows good academic practice was developed and followed throughout the development of this thesis.

Objective 4. Develop a framework as an artefact that permits its evaluation in terms of applicability, quality, efficiency, and efficacy aimed to demonstrate its feasibility to solve the business problem.

The introduced framework was developed and delineated as a specific artefact that allows its evaluation with respect to its organisational applicability, quality, efficiency, and efficacy.

Objective 5. Validate the framework in real-world scenarios.

The framework items were validated in extensive expert workshops and the framework was subsequently adapted and improved to incorporate expert feedback.

Objective 6. Evaluate the proposed framework and compare it with related research contributions in the area and other existing approaches in the industry.

The framework has been evaluated in two highly relevant case studies and the evaluation results were discussed in the context of related research contributions and compliance approaches in the industry.

8.2 Main contributions

The main contributions of this work can be summarized as follows:

1. The thesis includes a state-of-the-art analysis of relevant approaches from the areas of change management, outsourcing and cloud services, compliance requirements, frameworks and their success factors, and legal environment for compliance and these approaches have been assessed, discussed and structured. This is a solid foundation for future research endeavours in the area.
2. The motivation that has been provided for the development of the framework presents a good overview of needs and demands in the area of change management in the context of CC and outsourcing. Reasons have been solicited from the point of view of current computer science and information systems research, from the point of view of predominant paradigms in the area of management standards for information management, as well as from the point of view of mapping approaches for management and process standards.
3. The presented questionnaires in the different areas of the framework allow a holistic and cross-disciplinary assessment of compliance aspects associated with CC and outsourcing.
4. The processes and definitions of protection categories within the framework provide a blueprint for the integration of GRC aspects in organisational change management.
5. The validation of the different framework items demonstrates the relevance of the topics of this thesis in the industry.
6. The evaluation of the framework in two real-world scenarios provides a proof of the applicability and adaptability of the framework.

8.3 Benefits of the Proposed Framework

The benefits the framework provides can be summarised in the following statement: the proposed framework provides a holistic compliance approach to change management in CC and outsourcing scenarios that integrates organisational, technological, legal, and cultural aspects.

More specifically, the benefits are:

1. The framework provides a blueprint for making the change management function of an organisation compliant with a wide area of requirements coming from diverse problem domains (e.g., technological and legal).

2. The modular approach of the framework makes a gradual introduction with only one or some of the specified problem domains considered a relevant option.
3. Furthermore, the modular approach allows both the extension of the framework with requirements from new problem domains (e.g., specific sectoral requirements such as healthcare), as well as the adaptation of existing questionnaires to specifics of diverging problem domains (e.g., national peculiarities in legal requirements).
4. The expert validation demonstrates that the framework was met with a good degree of acceptance by leading practitioners in the field.
5. The evaluation approach can serve as a guide for the introduction of the framework in new organisations.

8.4 Critical Reflection and Lessons Learned

When planning an endeavour with the complexity and effort of a thesis work most plans that were set out at the beginning need adaptations to account for unexpected outcomes and changes in the environment of the work. This was also the case with this work. Based on the decade-long experience of the author as an expert and decision maker in the GRC field, some early expectations about the process of developing the framework were somewhat more optimistic. Recognising the relevance of the framework from a pragmatic, industry-driven point of view, the author had to dive deep and conduct several workshops with the supervisors in order to establish a solid understanding of how to address and prepare the motivation in the background section. The state-of-the-art in the relevant areas is developing faster and faster. While this may serve as a proof about the foresight to select a topic with a growing relevance that is “cutting-edge”, it also required several periodic updates of the background section in order to reflect developments that emerged worldwide during the development, validation, and evaluation of the framework.

This duality of core science and research and its application in real life scenarios is maybe the main defining characteristic of the work. The framework is not a purely scientific tool, intended for laboratory experiments. It lives from the constant interaction with actual organisations and their “pain points” are reflected in their structure and paradigms. On the other side, it is not simply a management tool that an organisation can apply “out-of-the-box” as its usage requires understanding the background of technological, legal, organisational, and cultural aspects.

8.5 Potentials for Future Applications and Further Development of the Framework

The already stated modular structure of the framework makes it also a good starting point for future applications and further development. As currently more and more traditional business models are being "digitalised" and CC and outsourcing are the typical approaches how this is being done, there are growing potentials to apply the framework in this context. Previously, when IT was regarding as a more or less supporting function within an organisation, GRC aspects of IT were considered an IT problem. Today, when IT drives bigger and bigger shares of daily business and is regarding as an important differentiating factor for future growth and value creation, the GRC aspects of IT are becoming the most important ones.

Thus, extended opportunities for future applications lie in sectors that are becoming increasingly "digital" and are subjected to more stringent regulations. Examples include the banking and the financial sector, as well as the healthcare sector. The advent of smart autonomous vehicles that integrate also external cloud services as part of their value proposition makes the framework also relevant for car manufacturers. Furthermore, business and service provision models in transportation that will increasingly rely on such vehicles also need to address GRC aspects which makes the framework a viable choice for operators in this area. The advent of the fourth industrial revolution increases the relevance of the framework in this area too.

Finally, the increase of regulations and public scrutiny in various industry sectors that started after the financial crisis of 2008-2009 leads to an increasing demand for holistic and working GRC approaches such as the developed framework.

8.6 Outlook on Future Research Activities in the Area

Based on the potentials of the framework and the state-of-the-art research in the relevant areas the following lines of future research can be envisioned.

In the first line of research, extensions and adaptations of the framework for various application scenarios can be developed, applied and evaluated. Currently, the author is considering such research activities in cooperation with one of the world-leading compliance and auditing companies.

In the second line of research fall topics of mapping the framework to various methods and standards in the industry. Examples include COBIT, ITIL and various ISO standards such as ISO 38 500, ISO 20 000 and ISO 27001. This path will lead us to new conclusions and synergies with well stablished initiatives.

The third line of research is building on the first one and will comprise of cross-sectoral and cross-national comparisons of the performance of the framework in different organisations where it has been applied.

9 References

Abdullah, N. S., Indulska, M., & Sadiq, S. (2016). Compliance management ontology – a shared conceptualization for research and practice in compliance management. *Information Systems Frontiers*, *18*(5), 995–1020. https://doi.org/10.1007/s10796-016-9631-4

Abdullah, N. S., Sadiq, S., & Indulska, M. (2010). Emerging challenges in information systems research for regulatory compliance management. In *Advanced information systems engineering* (pp. 251–265).

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Prentice-Hall.

Akande, A. O., April, N. A., & Van Belle, J.-P. (2013). Management Issues with Cloud Computing. In *Proceedings of the Second International Conference on Innovative Computing and Cloud Computing* (pp. 119:119–119:124). New York, NY, USA: ACM. https://doi.org/10.1145/2556871.2556899

Aladwani, A. M. (2001). Change management strategies for successful ERP implementation. *Business Process Management Journal*, *7*(3), 266–275.

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, *305*, 357–383. https://doi.org/10.1016/j.ins.2015.01.025

Alreemy, Z., Chang, V., Walters, R., & Wills, G. (2016). Critical success factors (CSFs) for information technology governance (ITG). *International Journal of Information Management*, *36* (6, Part A), 907–916. https://doi.org/10.1016/j.ijinfomgt.2016.05.017

Ang, S., Joseph, D., & Slaughter, S. A. (2015). IT Professionals and the IT Profession. In *Wiley Encyclopedia of Management*. John Wiley & Sons, Ltd.

Reed, A., Rezek, C., & Simmonds, P. (2011). Security Guidance for Critical Areas of Focus in Cloud Computing. Cloud Security Alliance (CSA). Retrieved from http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., … Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50–58. https://doi.org/http://doi.acm.org/10.1145/1721654.1721672

Avison, D., Jones, J., Powell, P., & Wilson, D. (2004). Using and validating the strategic alignment model. *The Journal of Strategic Information Systems*, *13*(3), 223–246.

Bartens, Y., Schulte, F., & Voß, S. (2014). Business/IT Alignment in Two Sided Markets: A Study of COBIT 5 for Internet Based Business Models. *International Journal of IT/Business Alignment and Governance (IJITBAG)*, *5*(2), 27–43. https://doi.org/10.4018/ijitbag.2014070102

Baskerville, R. L., & Myers, M. D. (2015). Design ethnography in information systems. *Information Systems Journal*, *25*(1), 23–46. https://doi.org/10.1111/isj.12055

Baxter, R. J., Holderness, D. K., & Wood, D. A.2016). Applying Basic Gamification Techniques to IT Compliance Training: Evidence from the Lab and Field. *Journal of Information Systems*, *30*(3), 119–133. https://doi.org/10.2308/isys-51341

Becker, J., & Bailey, E. (2014). A Comparison of IT Governance & Control Frameworks in Cloud Computing. *AMCIS 2014 Proceedings*. Retrieved from http://aisel.aisnet.org/amcis2014/ISSecurity/GeneralPresentations/4

Bergvall-Kåreborn, B., & Howcroft, D. (2014). Persistent problems and practices in information systems development: a study of mobile applications development and distribution. *Information Systems Journal*, *24*(5), 425–444. https://doi.org/10.1111/isj.12036

Bhamidipaty, A., Narendra, N. C., Nagar, S., Varshneya, V. K., Vasa, M., & Deshwal, C. (2009). Indra: An integrated quantitative system for compliance management for IT service delivery. *IBM Journal of Research and Development*, *53*(6), 6:1–6:12. https://doi.org/10.1147/JRD.2009.5429034

Bhattacherjee, A., & Park, S. C. (2014). Why end-users move to the cloud: a migration-theoretic analysis. *European Journal of Information Systems*, 23(3), 357-372. https://doi.org/10.1057/ejis.2013.1

Bin-Abbas, H., & Bakry, S. H. (2014). Assessment of IT governance in organizations: A simple integrated approach. *Computers in Human Behavior*, *32*, 261–267. https://doi.org/10.1016/j.chb.2013.12.019

Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). Validation in Information Systems Research: A State-of-the-art Assessment. *Management Information Systems Quarterly*, *25*(1), 1–16. https://doi.org/10.2307/3250956

Breaux, T. D., Antón, A. I., Boucher, K., & Dorfman, M. (2009). IT Compliance: Aligning Legal and Product Requirements. *IT Professional*, *11*(5), 54–58.

Brehmer, M., & Seitz, J. (2015). Long-term Data Security Challenges Using Cloud Storage Services. *WHICEB 2015 Proceedings*. Retrieved from http://aisel.aisnet.org/whiceb2015/21

Brender, N., & Markov, I. (2013). Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. *International Journal of Information Management*, *33*(5), 726–733.

Broman Toft, M., Schuitema, G., & Thøgersen, J. (2014). Responsible technology acceptance: Model development and application to consumer acceptance of Smart Grid technology. *Applied Energy*, *134*, 392–400. https://doi.org/10.1016/j.apenergy.2014.08.048

Brown, B. (2009). Introduction to SOA governance and service lifecycle management. Retrieved from ftp://ftp.software.ibm.com/software/soa/pdf/IBMSGMMOverview.pdf

Buchwald, A., Urbach, N., & Ahlemann, F. (2014). Business value through controlled IT: toward an integrated model of IT governance success and its impact. *Journal of Information Technology*, *29*(2), 128–147. https://doi.org/10.1057/jit.2014.3

Buckl, S., Ernst, A. M., Lankes, J., Matthes, F., & Schweda, C. M. (2008). Enterprise architecture management patterns–exemplifying the approach. In *Enterprise Distributed Object Computing Conference, 2008. EDOC'08. 12th International IEEE* (pp. 393–402). IEEE.

By, R. T. (2005). Organisational change management: A critical review. *Journal of Change Management*, *5*(4), 369–380. https://doi.org/10.1080/14697010500359250

Calvo-Manzano, J. A., Agustín, G. C., & Gilabert, T. S. F. (2008). Project Management Similarity Study: Experiment on Project Planning Practices Based on CMMI-Dev v1.2. In *EuroSPI* (Vol. 2008, pp. 1113–1123). Springer.

Casado-Lumbreras, C., Colomo-Palacios, R., Gomez-Berbis, J. M., & Garcia-Crespo, A. (2009). Mentoring programmes: a study of the Spanish software industry. *International Journal of Learning and Intellectual Capital*, *6*(3), 293–302. http://dx.doi.org/10.1504/IJLIC.2009.025046

Casado-Lumbreras, C., Colomo-Palacios, R., Hernández-López, A., & Soto-Acosta, P. (2011). Personnel Performance Appraisal Coverage in ITIL, COBIT and CMMi: A Study from the Perspective of People-CMM. *International Journal of Knowledge Society Research*, *2*(2), 59–70. http://dx.doi.org/10.4018/jksr.2011040106

Casado-Lumbreras, C., Colomo-Palacios, R., Ogwueleka, F. N., & Misra, S. (2014). Software Development Outsourcing: Challenges and Opportunities in Nigeria. *Journal of Global Information Technology Management*, *17*(4), 267–282. https://doi.org/10.1080/1097198X.2014.978626

Casado-Lumbreras, C., Colomo-Palacios, R., Soto-Acosta, P., & Misra, S. (2011). Culture dimensions in software development industry: The effects of mentoring. *Scientific Research and Essays*, *6*(11), 2403–2412.

Catteddu, D. (2010). *Cloud Computing: benefits, risks and recommendations for information security*. Springer.

Chang, S.-I. (2005). An alternative methodology for Delphi-type research in IS key issues studies. *International Journal of Management and Enterprise Development*, *3*(1-2), 147–168. https://doi.org/10.1504/IJMED.2006.008247

Chang, V., Bacigalupo, D., Wills, G., & De Roure, D. (2010). A categorisation of cloud computing business models. In *Proceedings of the 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing* (pp. 509–512).

Chang, V., Kuo, Y.-H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems*, *57*, 24–41.

Chang, V., & Ramachandran, M. (2016). Towards Achieving Data Security with the Cloud Computing Adoption Framework. *IEEE Transactions on Services Computing*, *9*(1), 138–151. https://doi.org/10.1109/TSC.2015.2491281

Chang, V., Walters, R. J., & Wills, G. (2013). The development that leads to the Cloud Computing Business Framework. *International Journal of Information Management*, *33*(3), 524–538.

Chan, H., & Chieu, T. (2010). Ranking and mapping of applications to cloud computing services by SVD. In *Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP* (pp. 362–369). IEEE.

Chatterjee, S. (2010). *Design research in information systems: theory and practice* (Vol. 22). Springer.

Chaudhuri, A. (2015). Governance and Risk Management in the Cloud with Cloud Controls Matrix V3 and ISO/IEC 38500:2008. In K. Munir, M. S. Al-Mutairi, & L. A. Mohammed (Eds.), *Handbook of Research on Security Considerations in Cloud Computing*. IGI Global.

Chazalet, A. (2010a). Service level agreements compliance checking in the cloud computing: architectural pattern, prototype, and validation. In *Software Engineering Advances (ICSEA), 2010 Fifth International Conference on* (pp. 184–189). IEEE.

Chazalet, A. (2010b). Service level checking in the cloud computing context. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on* (pp. 297–304). IEEE.

Cheung, R., & Vogel, D. (2013). Predicting user acceptance of collaborative technologies: An extension of the technology acceptance model for e-learning. *Computers & Education*, *63*, 160–175. https://doi.org/10.1016/j.compedu.2012.12.003

Choi, J., Nazareth, D. L., & Jain, H. K. (2013). The Impact of SOA Implementation on IT-Business Alignment: A System Dynamics Approach. *ACM Transactions on*

Management Information Systems, *4*(1), 3:1–3:22. https://doi.org/10.1145/2445560.2445563

Choi, K. S., Im, I., & Hofstede, G. J. (2016). A cross-cultural comparative analysis of small group collaboration using mobile twitter. *Computers in Human Behavior*, *65*, 308–318. https://doi.org/10.1016/j.chb.2016.08.043

Choi, Y. B., Capitan, K. E., Krause, J. S., & Streeper, M. M. (2006). Challenges associated with privacy in health care industry: implementation of HIPAA and the security rules. *Journal of Medical Systems*, *30*(1), 57–64.

Chou, D. C. (2015). Cloud computing: A value creation model. *Computer Standards & Interfaces*, *38*, 72–77. https://doi.org/10.1016/j.csi.2014.10.001

Chou, T.-C., & Liao, J.-L. (2015). IT governance balancing global integration and local responsiveness for multinational companies. *Total Quality Management & Business Excellence*, *0*(0), 1–15. https://doi.org/10.1080/14783363.2015.1049145

CMMI Product Team. (2010). *CMMI for Service, Version 1.3, CMMI-SVC v1. 3*. CMU/SEI-2010-TR-034, Technical report, Software Engineering Institute.

Colomo-Palacios, R., Casado-Lumbreras, C., Soto-Acosta, P., García-Peñalvo, F. J., & Tovar-Caro, E. (2013). Competence gaps in software personnel: A multi-organizational study. *Computers in Human Behavior*, *29*(2), 456–461. https://doi.org/10.1016/j.chb.2012.04.021

Colomo-Palacios, R., Fernandes, E., Sabbagh, M., & de Amescua Seco, A. (2012). Human and intellectual capital management in the cloud: software vendor perspective. *Journal of Universal Computer Science*, *18*(11), 1544–1557.

Colomo-Palacios, R., Tovar-Caro, E., García-Crespo, Á., & Gómez-Berbís, J. M. (2010). Identifying technical competences of IT Professionals: the case of software engineers. *International Journal of Human Capital and Information Technology Professionals*, *1*(1), 31–43.

Connolly, L., & Lang, M. (2012). Investigation of cultural aspects within information systems security research. In *Internet Technology And Secured Transactions, 2012 International Conference for* (pp. 105–111).

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Cruzes, D. S., Dybå, T., Runeson, P., & Höst, M. (2014). Case studies synthesis: a thematic, cross-case, and narrative synthesis worked example. *Empirical Software Engineering*, *20*(6), 1634–1665. https://doi.org/10.1007/s10664-014-9326-8

Dahlberg, T., Hokkanen, P., & Newman, M. (2016). How Business Strategy and Technology Impact the Role and the Tasks of CIOs: An Evolutionary Model. *International Journal of IT/Business Alignment and Governance (IJITBAG)*, *7*(1), 1–19. https://doi.org/10.4018/IJITBAG.2016010101

Damianides, M. (2005). Sarbanes-Oxley and IT governance: New guidance on IT control and compliance. *Information Systems Management*, *22*(1), 77–85.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *Management Information Systems Quarterly*, *13*(3), 319–340.

De Haes, S., Huygh, T., Joshi, A., & Van Grembergen, W. (2016). Adoption and Impact of IT Governance and Management Practices: A COBIT 5 Perspective. *International Journal of IT/Business Alignment and Governance*, *7*(1), 50–72. https://doi.org/10.4018/IJITBAG.2016010104

Delbecq, A. L., Van de Ven, A. H., & Gustafson, D. H. (1975). *Group techniques for program planning: A guide to nominal group and Delphi processes*. Scott Foresman.

DeLuccia IV, J. J. (2008). *IT compliance and controls: Best practices for implementation*. John Wiley & Sons.

Dubé, L., & Paré, G. (2003). Rigor in Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations. *Management Information Systems Quarterly*, *27*(4), 597–635.

Duggan, E. W., & Thachenkary, C. S. (2004). Integrating nominal group technique and joint application development for improved systems requirements determination. *Information & Management*, *41*(4), 399–411. https://doi.org/10.1016/S0378-7206(03)00080-6

Dutta, A., Peng, G., & Choudhary, A. (2013). Risks in enterprise cloud computing: the perspective of IT experts. *Journal of Computer Information Systems*, *53*(4), 39–48.

Dzombeta, S., Stantchev, V., Colomo-Palacios, R., Brandis, K., & Haufe, K. (2014). Governance of Cloud Computing Services for the Life Sciences. *IT Professional*, *16*(4), 30–37. http://dx.doi.org/10.1109/MITP.2014.52

Earl, M. J., Sampler, J. L., & Short, J. E. (1995). Strategies for business process reengineering: evidence from field studies. *Journal of Management Information Systems*, *12*(1), 31–56.

El-Gazzar, R., Hustad, E., & Olsen, D. H. (2016). Understanding cloud computing adoption issues: A Delphi study approach. *Journal of Systems and Software*, *118*, 64–84. https://doi.org/10.1016/j.jss.2016.04.061

Elliott, T. R., & Shewchuk, R. M. (2002). Using the Nominal Group Technique to Identify the Problems Experienced by Persons Living with Severe Physical Disabilities. *Journal of Clinical Psychology in Medical Settings*, *9*(2), 65–76. https://doi.org/10.1023/A:1014931924809

Karanja, E., & Zaveri, J. (2014). Ramifications of the Sarbanes Oxley (SOX) Act on IT governance. *International Journal of Accounting & Information Management*, *22*(2), 134–145. https://doi.org/10.1108/IJAIM-02-2013-0017

Ferris, C., & Farrell, J. (2003). What are Web services? *Communications of the ACM*, *46*(6), 31. https://doi.org/http://doi.acm.org/10.1145/777313.777335

Franz, T. M., & Larson, J. R. (2002). The impact of experts on information sharing during group discussion. *Small Group Research*, *33*(4), 383–411.

Freimut, B., Briand, L. C., & Vollei, F. (2005). Determining inspection cost-effectiveness by combining project data and expert opinion. *IEEE Transactions on Software Engineering*, *31*(12), 1074–1092. https://doi.org/10.1109/TSE.2005.136

Frick, H.-J. (2012). Deutsche Post: Optimierung der Geschäftsprozesse in der Kommunalverwaltung durch Digitales Schriftgutmanagement. In *Prozessmanagement individuell umgesetzt* (pp. 153–171). Springer.

Galup, S. D., Dattero, R., Quan, J. J., & Conger, S. (2009). An Overview of IT Service Management. *Communications of the ACM*, *52*(5), 124–127. https://doi.org/10.1145/1506409.1506439

Gama, N., Nunes da Silva, R., & Mira da Silva, M. (2011). Using People-CMM for Diminishing Resistance to ITIL. *International Journal of Human Capital and Information Technology Professionals (IJHCITP)*, *2*(3), 29–43.

Garg, S. K., Versteeg, S., & Buyya, R. (2013). A framework for ranking of cloud computing services. *Future Generation Computer Systems*, *29*(4), 1012–1023.

Garrison, G., Kim, S., & Wakefield, R. L. (2012). Success Factors for Deploying Cloud Computing. *Communications of the ACM*, *55*(9), 62–68. https://doi.org/10.1145/2330667.2330685

Garrison, G., Wakefield, R. L., & Kim, S. (2015). The effects of IT capabilities and delivery model on cloud computing success and firm performance for cloud supported processes and operations. *International Journal of Information Management*, *35*(4), 377–393. https://doi.org/10.1016/j.ijinfomgt.2015.03.001

Gartner. (2016). Gartner Says By 2020, a Corporate. Retrieved September 30, 2016, from http://www.gartner.com/newsroom/id/3354117

Garvin, D. A. (2000). *Learning in action: A guide to putting the learning organization to work*. Harvard Business Press.

Gerow, J. E., Grover, V., Thatcher, J., & Roth, P. (2014). Looking Toward the Future of IT-Business Strategic Alignment through the Past: A Meta-Analysis. *Management Information Systems Quarterly*, *38*(4), 1059–1085.

Goldkuhl, G. (2011). Pragmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems*, *21*(2), 135–146. https://doi.org/10.1057/ejis.2011.54

Grembergen, W. V. (Ed.). (2003). *Strategies for Information Technology Governance*. Hershey, PA, USA: IGI Publishing.

Grönroos, C. (1984). A service quality model and its marketing implications. *European Journal of Marketing*, *18*(4), 36–44.

Grover, V., Jeong, S. R., Kettinger, W. J., & Teng, J. T. (1995). The implementation of business process reengineering. *Journal of Management Information Systems*, *12*(1), 109–144.

Hall, E. T. (1977). *Beyond Culture*. New York: Anchor Books.

Hall, M. E. (2009). Pioneers of the Private Cloud. *Computerworld*, 14–19.

Hamdaqa, M., & Hamou-Lhadj, A. (2011). An approach based on citation analysis to support effective handling of regulatory compliance. *Future Generation Computer Systems*, *27*(4), 395–410.

Harris, J., & Cummings, M. (2007). Compliance issues and IS degree programs. *Journal of Computing Sciences in Colleges*, *23*(1), 14–20.

Hasse, L. (2012). Umsetzung der „Orientierungshilfe Krankenhausinformationssysteme “in Thüringen. *Datenschutz Und Datensicherheit-DuD*, *36*(8), 560–560.

Havelka, D., & Merhout, J. W. (2013). Internal information technology audit process quality: Theory development using structured group processes. *International Journal of Accounting Information Systems*, *14*(3), 165–192. https://doi.org/10.1016/j.accinf.2012.12.001

Hayden, L. (2009). Designing common control frameworks: A model for evaluating information technology governance, risk, and compliance control rationalization strategies. *Information Security Journal: A Global Perspective*, *18*(6), 297–305.

Health Information Privacy. (n.d.). [Government]. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/

Health Information Technology for Economic and Clinical Health (HITECH), Act. FedReg 160: Health Insurance Reform: Security Standards (2009).

Heiser, J. (2009). What You Need to Know About Cloud Computing Security and Compliance. Retrieved October 4, 2016, from https://www.gartner.com/doc/1071415/need-know-cloud-computing-security

Henderson, J. C., & Venkatraman, N. (1992). *Strategic alignment: a model for organizational transformation through information technology*. Oxford University Press, New York.

Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, *32*(1), 4–16.

Herold, R., & Beaver, K. (2004). *The practical guide to HIPAA privacy and security compliance*. CRC Press.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *Management Information Systems Quarterly*, *28*(1), 75–106.

Hofstede, G. (1983a). The cultural relativity of organizational practices and theories. *Journal of International Business Studies*, 75–89.

Hofstede, G. (1983b). The cultural relativity of organizational practices and theories. *Journal of International Business Studies*, *14*(2), 75–89.

Hofstede, G. (1984). Cultural dimensions in management and planning. *Asia Pacific Journal of Management*, *1*(2), 81–99.

Hofstede, G. (2003). *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations* (2nd edition). Thousand Oaks, Calif.: SAGE Publications, Inc.

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and Organizations: Software of the Mind, Third Edition* (3 edition). New York: McGraw-Hill Education.

Horton, J. (1980). Nominal group technique. *Anaesthesia*, *35*(8), 811–814.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management*, *49*(2), 99–110. https://doi.org/10.1016/j.im.2011.12.005

Hsu, W.-H. L. (2012). Conceptual Framework of Cloud Computing Governance Model–An Education Perspective. *IEEE Technology and Engineering Education (ITEE)*, *7*(2), 3.

IBM. (2006). SOA Governance and Service Lifecycle Management. Retrieved from http://www-01.ibm.com/software/solutions/soa/gov/

Jäntti, M., & Hotti, V. (2016). Defining the relationships between IT service management and IT service governance. *Information Technology and Management*, *17*(2), 141–150. https://doi.org/10.1007/s10799-015-0239-z

Jaster, B., Mendonca, J. C. de, Slamka, C., & Radmacher, M. (2010). *Wer klaut in der Cloud?* Bonn, Germany: Detecon International GmbH.

Jiménez-Domingo, E., Gómez-Berbís, J. M., Colomo-Palacios, R., & García-Crespo, Á. (2011). CARL: A Complex Applications Interoperability Language based on Semantic Technologies for Platform-as-a-Service Integration and Cloud Computing. *Journal of Research and Practice in Information Technology*, *43*(3), 227.

Joha, A., & Janssen, M. (2012). Transformation to cloud services sourcing: required it governance capabilities. *ICST Transactions on E-Business*, *12*(7-9), 5.

Joo, J., & Sang, Y. (2013). Exploring Koreans' smartphone usage: An integrated model of the technology acceptance model and uses and gratifications theory. *Computers in Human Behavior*, *29*(6), 2512–2518. https://doi.org/10.1016/j.chb.2013.06.002

JPC Rodrigues, J., de la Torre, I., Fernandez, G., & Lopez-Coronado, M. (2013). Analysis of the Security and Privacy Requirements of Cloud-Based Electronic

Health Records Systems. *Journal of Medical Internet Research*, *15*(8), E186. https://doi.org/10.2196/jmir.2494

Juan Carlos I. LOPD, Ley Orgánica Protección de Datos de Carácter Personal § BOE nº 298 (1999).

Juiz, C., & Toomey, M. (2015). To Govern IT, or Not to Govern IT? *Communications of the ACM*, *58*(2), 58–64. https://doi.org/10.1145/2656385

Julisch, K., & Hall, M. (2010). Security and control in the cloud. *Information Security Journal: A Global Perspective*, *19*(6), 299–309.

Kaidalova, J., Siegerroth, U., Bukowska, E., & Shilov, N. (2014). Enterprise Modeling for Business and IT Alignment: Challenges and Recommendations. *International Journal of IT/Business Alignment and Governance (IJITBAG)*, *5*(2), 44–69. https://doi.org/10.4018/ijitbag.2014070103

Kalinowski, M., Biffl, S., Spínola, R. O., & Reinehr, S. (2014). From project-oriented to service-oriented software development: an industrial experience guided by a service reference model. *Journal of Software Engineering Research and Development*, *2*(1). https://doi.org/10.1186/s40411-014-0010-x

Kaplan, B., & Duchon, D. (1988). Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study. *Management Information Systems Quarterly*, *12*(4), 571–586. https://doi.org/10.2307/249133

Kasvi, J. J. J., Vartiainen, M., Pulkkis, A., & Nieminen, M. (2000). The role of information support systems in the joint optimization of work systems. *Human Factors and Ergonomics in Manufacturing & Service Industries*, *10*(2), 193–221. https://doi.org/10.1002/(SICI)1520-6564(200021)10:2<193::AID-HFM5>3.0.CO;2-H

Khanagha, S., Volberda, H., Sidhu, J., & Oshri, I. (2013). Management innovation and adoption of emerging technologies: The case of cloud computing. *European Management Review*, *10*(1), 51–67.

Kim, S. (2007). IT compliance of industrial information systems: Technology management and industrial engineering perspective. *Journal of Systems and Software*, *80*(10), 1590–1593.

Kim, W. (2011). Cloud computing adoption. *International Journal of Web and Grid Services*, *7*(3), 225–245.

Kluckhohn, F. R., & Strodtbeck, F. L. (1961). *Variations in Value Orientations*. Row, Peterson.

Koetter, F., Kochanowski, M., Renner, T., Fehling, C., & Leymann, F. (2013). Unifying Compliance Management in Adaptive Environments through Variability Descriptors (Short Paper). In *2013 IEEE 6th International Conference on Service-Oriented Computing and Applications* (pp. 214–219). https://doi.org/10.1109/SOCA.2013.23

Krallmann, H., Schröpfer, C., Stantchev, V., & Offermann, P. (2008). Enabling Autonomous Self-optimization in Service-oriented Systems. In *Proceedings of The 8th International Workshop on Autonomous Systems - Self Organisation, Management and Control* (pp. 127–134). Berlin, New York: Springer.

Kshetri, N. (2013). IT in the Chinese Healthcare Industry. *IT Professional*, *15*(1), 12–15. https://doi.org/10.1109/MITP.2013.14

Kshetri, N., & Murugesan, S. (2013). Cloud Computing and EU Data Privacy Regulations. *Computer*, *46*(3), 86–89.

Kundu, G. K., & Manohar, B. M. (2012). A unified model for implementing lean and CMMI for Services (CMMI-SVC v1.3) best practices. *Asian Journal on Quality*, *13*(2), 138–162. https://doi.org/10.1108/15982681211265463

Laatikainen, G., Mazhelis, O., & Tyrvainen, P. (2016). Cost benefits of flexible hybrid cloud storage: Mitigating volume variation with shorter acquisition cycle. *Journal of Systems and Software*, *122*, 180–201. https://doi.org/10.1016/j.jss.2016.09.008

Larrucea, X., O'Connor, R. V., Colomo-Palacios, R., & Laporte, C. Y. (2016). Software Process Improvement in Very Small Organizations. *IEEE Software*, *33*(2), 85–89. https://doi.org/10.1109/MS.2016.42

Larrucea, X., Santamaría, I., & Colomo-Palacios, R. (2016). Assessing ISO/IEC29110 by means of ITMark: results from an experience factory. *Journal of Software: Evolution and Process,* *28*(11), 969-980. http://dx.doi.org/10.1002/smr.1795

Law, C. C., & Ngai, E. W. (2007). ERP systems adoption: An exploratory study of the organizational factors and impacts of ERP success. *Information & Management*, *44*(4), 418–432.

Lawler, J., Joseph, A., & Howell-Barber, H. (2012). A Case Study Of Determinants Of An Effective Cloud Computing Strategy. *Review of Business Information Systems (RBIS)*, *16*(3), 145–156.

Lawton, R. (2007). Transitioning IT From a Compliance to a Value-driven Enterprise Using COBIT. *Information Systems Control Journal*, *6*, 43.

Lederer, A. L., & Mendelow, A. L. (1986). Issues in information systems planning. *Information & Management*, *10*(5), 245–254. https://doi.org/10.1016/0378-7206(86)90027-3

Leichter, W. (2014). Enabling the Cloud by Protecting Sensitive Data. Presented at the INTEROP 2014. Retrieved from http://presentations.interop.com/events/las-vegas/2014/open-to-all---keynote-presentations/download/1643

Leidner, D. E., & Kayworth, T. (2006). Review: a review of culture in information systems research: toward a theory of information technology culture conflict. *Management Information Systems Quarterly*, *30*(2), 357–399.

Lema, L., Calvo-Manzano, J.-A., Colomo-Palacios, R., & Arcilla, M. (2015). ITIL in small to medium-sized enterprises software companies: towards an implementation sequence. *Journal of Software: Evolution and Process*, *27*(8), 528–538. https://doi.org/10.1002/smr.1727

Lepmets, M., Cater-Steel, A., Gacenga, F., & Ras, E. (2012). Extending the IT service quality measurement framework through a systematic literature review. *Journal of Service Science Research*, *4*(1), 7–47. https://doi.org/10.1007/s12927-012-0001-6

Liang, H., Xue, Y., & Wu, L. (2013). Ensuring Employees' IT Compliance: Carrot or Stick? *Information Systems Research*, *24*(2), 279–294. https://doi.org/10.1287/isre.1120.0427

Lincoln, Y. S., Lynham, S. A., & Guba, E. G. (2011). Paradigmatic controversies, contradictions, and emerging confluences, revisited. *The Sage Handbook of Qualitative Research*, *4*, 97–128.

Liu, S. (2012). New Perspectives for IT. *IT Professional*, *14*(1), 2–4. https://doi.org/10.1109/MITP.2012.15

Lombardi, R., Giudice, M. D., Caputo, A., Evangelista, F., & Russo, G. (2015). Governance and Assessment Insights in Information Technology: the Val IT Model. *Journal of the Knowledge Economy*, *7*(1), 292–308. https://doi.org/10.1007/s13132-015-0328-6

Lowry, P. B., & Wilson, D. (2016). Creating agile organizations through IT: The influence of internal IT service perceptions on IT service quality and IT agility. *The Journal of Strategic Information Systems*, *25*(3), 211–226. https://doi.org/10.1016/j.jsis.2016.05.002

Luftman, J. (2003). Assessing It/Business Alignment. *Information Systems Management*, *20*(4), 9–15. https://doi.org/10.1201/1078/43647.20.4.20030901/77287.2

Luftman, J., Lyytinen, K., & Zvi, T. ben. (2015). Enhancing the measurement of information technology (IT) business alignment and its influence on company performance. *Journal of Information Technology*. https://doi.org/10.1057/jit.2015.23

Luftman, J., Papp, R., & Brier, T. (1999). Enablers and Inhibitors of business-IT Alignment. *Communications of the AIS*, *1*(3), Article 1. Retrieved from http://dl.acm.org/citation.cfm?id=374122.374123

Mackintosh, A. R. (2008). The first electronic computer. *Physics Today*, *40*(3), 25–32.

Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does Sample Size Matter in Qualitative Research?: A Review of Qualitative Interviews in is Research. *Journal of Computer Information Systems*, *54*(1), 11–22. https://doi.org/10.1080/08874417.2013.11645667

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, *51*(1), 176–189.

Martens, B., & Teuteberg, F. (2012). Decision-making in cloud computing environments: A cost and risk based approach. *Information Systems Frontiers*, *14*(4), 871–893. https://doi.org/10.1007/s10796-011-9317-x

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud security and privacy: an enterprise perspective on risks and compliance*. O'Reilly.

Maznevski, M. L., Gomez, C. B., DiStefano, J. J., Noorderhaven, N. G., & Wu, P.-C. (2002). Cultural Dimensions at the Individual Level of Analysis The Cultural Orientations Framework. *International Journal of Cross Cultural Management*, *2*(3), 275–295.

McCafferty, D. (2010). Cloudy Skies: Public versus private option still up in the air. *Baselinemagazine*, 28–32.

McNaughton, B., Ray, P., & Lewis, L. (2010). Designing an evaluation framework for IT service management. *Information & Management*, *47*(4), 219–225. https://doi.org/10.1016/j.im.2010.02.003

Mekawy, M., Rusu, L., & Ahmed, N. (2009). Business and IT Alignment: An Evaluation of Strategic Alignment Models. *Best Practices for the Knowledge Society. Knowledge, Learning, Development and Technology for All*, 447–455.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (draft). *NIST Special Publication*, *800*(145), 7.

Mesquida, A. L., Mas, A., Amengual, E., & Calvo-Manzano, J. A. (2012). IT Service Management Process Improvement based on ISO/IEC 15504: A systematic review. *Information and Software Technology*, *54*(3), 239–247. https://doi.org/10.1016/j.infsof.2011.11.002

Meyer, M., Zarnekow, R., & Kolbe, L. M. (2003). IT-Governance. *Wirtschaftsinformatik*, *45*(4), 445–448.

Michelberger Jr, P., & Lábodi, C. (2012). After Information Security–Before a Paradigm Change (A Complex Enterprise Security Model). *Acta Polytechnica Hungarica*, *14*(1), 32–42.

Mills, S. (2007). IBM Software for SOA and Business Flexibility, 16.

Mingers, J. (2003). The paucity of multimethod research: a review of the information systems literature. *Information Systems Journal*, *13*(3), 233–249. https://doi.org/10.1046/j.1365-2575.2003.00143.x

Mokhtar, U. A., Yusof, Z. M., Ahmad, K., & Jambari, D. I. (2016). Development of function-based classification model for electronic records. *International Journal of Information Management*, *36*(4), 626–634. https://doi.org/10.1016/j.ijinfomgt.2016.04.009

Mora, M., Raisinghani, M., O’Connor, R. V., Marx-Gomez, J., & Gelman, O. (2014). An Extensive Review of IT Service Design in Seven International ITSM Processes Frameworks: Part I. *International Journal of Information Technologies and Systems Approach*, *7*(2), 83–107. https://doi.org/10.4018/ijitsa.2014070105

Moran, J. W., & Brightman, B. K. (2000). Leading organizational change. *Journal of Workplace Learning*, *12*(2), 66–74. https://doi.org/10.1108/13665620010316226

Moran, J. W., & Brightman, B. K. (2001). Leading organizational change. *Career Development International*, *6*(2), 111–119.

Myers, M. (1997). Qualitative Research in Information Systems. *Management Information Systems Quarterly*, *21*(2), 6.

Myers, M. D., & Tan, F. B. (2002). Beyond Models of National Culture in Information Systems Research. *Journal of Global Information Management (JGIM)*, *10*(1), 24–32. https://doi.org/10.4018/jgim.2002010103

Oates, B. J. (2005). *Researching Information Systems and Computing*. SAGE.

O’Connor, R.V., & Laporte, C. (2014). An innovative approach to the development of an international software process lifecycle standard for very small entities. *International Journal of Information Technologies and Systems Approach*, *7*(1), 1–22.

O’Connor, R. V., Raisinghani, M., Mora, M., Marx-Gomez, J., & Gelman, O. (2015). An Extensive Review of IT Service Design in Seven International ITSM Processes

Frameworks: Part II. *International Journal of Information Technologies and Systems Approach*, *8*(1), 69–90. https://doi.org/10.4018/ijitsa.2015010104

Olson, J. S., & Olson, G. M. (2003). Culture Surprises in Remote Software Development Teams. *Queue*, *1*(9), 52–59. https://doi.org/10.1145/966789.966804

Owens, D. (2010). Securing Elasticity in the Cloud. *Communications of the ACM*, *53*(6), 46–51. https://doi.org/10.1145/1743546.1743565

Padilla-Meléndez, A., del Aguila-Obra, A. R., & Garrido-Moreno, A. (2013). Perceived playfulness, gender differences and technology acceptance model in a blended learning scenario. *Computers & Education*, *63*, 306–317. https://doi.org/10.1016/j.compedu.2012.12.014

Panneerselvam, R. (2014). *Research methodology*. PHI Learning Pvt. Ltd.

Papanikolaou, N., Pearson, S., Mont, M. C., & Ko, R. K. L. (2014). A toolkit for automating compliance in cloud computing services. *International Journal of Cloud Computing*, *3*(1), 45–68. https://doi.org/10.1504/IJCC.2014.058830

Paré, G., Cameron, A.-F., Poba-Nzaou, P., & Templier, M. (2013). A systematic assessment of rigor in information systems ranking-type Delphi studies. *Information & Management*, *50*(5), 207–217. https://doi.org/10.1016/j.im.2013.03.003

Park, E., Baek, S., Ohm, J., & Chang, H. J. (2014). Determinants of player acceptance of mobile social network games: An application of extended technology acceptance model. *Telematics and Informatics*, *31*(1), 3–15. https://doi.org/10.1016/j.tele.2013.07.001

Park, E., & Kim, K. J. (2014). An Integrated Adoption Model of Mobile Cloud Services: Exploration of Key Determinants and Extension of Technology Acceptance Model. *Telematics and Informatics*, *31*(3), 376–385. https://doi.org/10.1016/j.tele.2013.11.008

Parsons, T., Shils, E. A., & Smelser, N. J. (1965). *Toward a general theory of action: Theoretical foundations for the social sciences*. Transaction Publishers.

Parthasarathy, S., & Sharma, S. (2014). Determining ERP customization choices using nominal group technique and analytical hierarchy process. *Computers in Industry*, *65*(6), 1009–1017. https://doi.org/10.1016/j.compind.2014.03.003

Pereira, R., Silva, M. M. da, & Lapão, L. V. (2014). Business/IT Alignment through IT Governance Patterns in Portuguese Healthcare. *International Journal of IT/Business Alignment and Governance (IJITBAG)*, *5*(1), 1–15. https://doi.org/10.4018/ijitbag.2014010101

Petruch, K., Stantchev, V., & Tamm, G. (2011). A survey on IT-governance aspects of cloud computing. *International Journal of Web and Grid Services*, *7*(3), 268–303.

Phillip J. Lageschulte et. al. (2011). IT Control Objectives for Cloud Computing. ISACA.

Pitropakis, N., Darra, E., Vrakas, N., & Lambrinoudakis, C. (2013). It’s All in the Cloud: Reviewing Cloud Security. In *Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on*

Autonomic and Trusted Computing (UIC/ATC) (pp. 355–362). https://doi.org/10.1109/UIC-ATC.2013.13

Pollard, C., & Cater-Steel, A. (2009). Justifications, Strategies, and Critical Success Factors in Successful ITIL Implementations in U.S. and Australian Companies: An Exploratory Study. *Information Systems Management*, *26*(2), 164–175. https://doi.org/10.1080/10580530902797540

Popović, K., & Hocenski, Z. (2010). Cloud computing security issues and challenges. In *2010 Proceedings of the 33rd International Convention MIPRO* (pp. 344–349).

Porter, M. (2001). The value chain and competitive advantage. *Understanding Business Processes, 1st Edn. Routledge (November 2000)*.

Porter, M. E., & Millar, V. E. (1985). *How information gives you competitive advantage*. Harvard Business Review, Reprint Service.

Prasad, A., & Green, P. (2015). Governing cloud computing services: Reconsideration of IT governance structures. *International Journal of Accounting Information Systems*, *19*, 45–58. https://doi.org/10.1016/j.accinf.2015.11.004

Prieto-González, L., Tamm, G., & Stantchev, V. (2015). Governance of cloud computing: semantic aspects and cloud service brokers. *International Journal of Web and Grid Services*, *11*(4), 377–389. https://doi.org/10.1504/IJWGS.2015.072806

Ragan, T. (2006). Keeping score in the IT compliance game. *Queue*, *4*(7), 38–43.

Rebollo, O., Mellado, D., & Fernández-Medina, E. (2012). A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment. *J. UCS*, *18*(6), 798–815.

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology*, *58*(0), 44 – 57. https://doi.org/http://dx.doi.org/10.1016/j.infsof.2014.10.003

Ridenour, C. S., & Newman. (2008). *Mixed Methods Research: Exploring the Interactive Continuum*. SIU Press.

Rimal, B. P., Jukan, A., Katsaros, D., & Goeleven, Y. (2011). Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach. *Journal of Grid Computing.*, *9*(1), 3–26. https://doi.org/10.1007/s10723-010-9171-y

Ruano-Mayoral, M., Casado-Lumbreras, C., Garbarino-Alberti, H., & Misra, S. (2014). Methodological framework for the allocation of work packages in global software development. *Journal of Software: Evolution and Process*, *26*(5), 476–487. https://doi.org/10.1002/smr.1618

Ruano-Mayoral, M., Colomo-Palacios, R., Fernández-González, J., & García-Crespo, Á. (2011). Towards a Framework for Work Package Allocation for GSD. In R. Meersman, T. Dillon, & P. Herrero (Eds.), *On the Move to Meaningful Internet Systems: OTM 2011 Workshops* (Vol. 7046, pp. 200–207). Springer Berlin / Heidelberg.

Runeson, P., & Höst, M. (2008). Guidelines for conducting and reporting case study research in software engineering. *Empirical Software Engineering*, *14*(2), 131–164. https://doi.org/10.1007/s10664-008-9102-8

Saeed, K. A., & Abdinnour, S. (2013). Understanding post-adoption IS usage stages: an empirical assessment of self-service information systems. *Information Systems Journal*, *23*(3), 219–244. https://doi.org/10.1111/j.1365-2575.2011.00389.x

Sanchez-Gordon, M.-L., O'Connor, R. V., & Colomo-Palacios, R. (2015). Evaluating VSEs Viewpoint and Sentiment Towards the ISO/IEC 29110 Standard: A Two Country Grounded Theory Study. In T. Rout, R. V. O'Connor, & A. Dorling (Eds.), *Software Process Improvement and Capability Determination* (pp. 114–127). Springer International Publishing.

Sarker, S., Xiao, X., & Beaulieu, T. (2013). Guest Editorial: Qualitative Studies in Information Systems: A Critical Review and Some Guiding Principles. *Management Information Systems Quarterly*, *37*(4), iii–xviii.

Schlarman, S. (2007). The IT Compliance Equation: Understanding the Elements. *EDPACS*, *35*(1), 12–24.

Schlosser, F., Beimborn, D., Weitzel, T., & Wagner, H.-T. (2015). Achieving social alignment between business and IT – an empirical evaluation of the efficacy of IT governance mechanisms. *Journal of Information Technology*, *30*(2), 119–135. https://doi.org/10.1057/jit.2015.2

Schneider, S., & Sunyaev, A. (2015). CloudLive: a life cycle framework for cloud services. *Electronic Markets*, *25*(4), 299–311. https://doi.org/10.1007/s12525-015-0205-y

Schröpfer, C. (2010). *Das SOA-Management-Framework: ein ganzheitliches, integriertes Konzept für die Governance Serviceorientierter Architekturen* (Vol. 13). GITO mbH Verlag.

Schweitzer, E. J. (2012). Reconciliation of the cloud computing model with US federal electronic health record regulations. *Journal of the American Medical Informatics Association*, *19*(2), 161–165. https://doi.org/10.1136/amiajnl-2011-000162

Seddon, J. J. M., & Currie, W. L. (2013). Cloud computing and trans-border health data: Unpacking U.S. and EU healthcare regulation and compliance. *Health Policy and Technology*. https://doi.org/10.1016/j.hlpt.2013.09.003

Sesay, A., & Ramirez, R. (2016). Theorizing the IT Governance Role in IT Sourcing Research. *AMCIS 2016 Proceedings*. Retrieved from http://aisel.aisnet.org/amcis2016/SCU/Presentations/15

Shannon, C. E., Weaver, W., & Wiener, N. (2009). The mathematical theory of communication. *Physics Today*, *3*(9), 31–32.

Shanteau, J. (1992). Competence in experts: The role of task characteristics. *Organizational Behavior and Human Decision Processes*, *53*(2), 252–266. https://doi.org/10.1016/0749-5978(92)90064-E

Sharifi, M., Ayat, M., Rahman, A. A., & Sahibudin, S. (2008). Lessons learned in ITIL implementation failure. In *Information Technology, 2008. ITSim 2008. International Symposium on* (Vol. 1, pp. 1–4). IEEE.

Shiau, W.-L., & Chau, P. Y. K. (2016). Understanding behavioral intention to use a cloud computing classroom: A multiple model comparison approach. *Information & Management*, *53*(3), 355–365. https://doi.org/10.1016/j.im.2015.10.004

Shilei, L., & Yong, W. (2009). Target-oriented obstacle analysis by PES^{TEL} modeling of energy efficiency retrofit for existing residential buildings in China's northern heating region. *Energy Policy*, *37*(6), 2098–2101.

Silverman, D. (1998). Qualitative research: meanings or practices? *Information Systems Journal*, *8*(1), 3–20. https://doi.org/10.1046/j.1365-2575.1998.00002.x

Simonsson, M., Johnson, P., & Ekstedt, M. (2010). The effect of IT governance maturity on IT governance performance. *Information Systems Management*, *27*(1), 10–24.

Sindre, G., & Opdahl, A. L. (2005). Eliciting security requirements with misuse cases. *Requirements Engineering*, *10*(1), 34–44.

Singh, S., & Sidhu, J. (2017). Compliance-based Multi-dimensional Trust Evaluation System for determining trustworthiness of Cloud Service Providers. *Future Generation Computer Systems*, *67*, 109–132. https://doi.org/10.1016/j.future.2016.07.013

Siurdyban, A. (2012). Understanding the IT/business partnership: A business process perspective. *Information Systems Frontiers*, *16*(5), 909–922. https://doi.org/10.1007/s10796-012-9388-3

Stantchev, V., Colomo-Palacios, R., & Niedermayer, M. (2014). Cloud Computing Based Systems for Healthcare. *The Scientific World Journal*, *2014*.

Stantchev, V., Colomo-Palacios, R., Soto-Acosta, P., & Misra, S. (2014). Learning management systems and cloud file hosting services: A study on students' acceptance. *Computers in Human Behavior*, *31*, 612–619. https://doi.org/10.1016/j.chb.2013.07.002

Stantchev, V., & Malek, M. (2011). Addressing Dependability throughout the SOA Life Cycle. *IEEE Transactions on Services Computing*, *4*(2), 85–95.

Stantchev, V., & Malek, M. (2011). Addressing Dependability throughout the SOA Life Cycle. *IEEE Transactions on Services Computing*, *4*(2), 85–95. https://doi.org/http://dx.doi.org/10.1109/TSC.2010.15

Stantchev, V., & Stantcheva, L. (2012). Extending Traditional IT-Governance Knowledge Towards SOA and Cloud Governance. *International Journal of Knowledge Society Research (IJKSR)*, *3*(2), 30–43.

Stantchev, V., & Stantcheva, L. (2013). Applying IT-Governance Frameworks for SOA and Cloud Governance. In *Information Systems, E-learning, and Knowledge Management Research* (pp. 398–407). Springer.

Stantchev, V., & Tamm, G. (2011). Addressing Non-Functional Properties of Services in IT Service Management. In *Non-Functional Properties in Service Oriented*

Architecture: Requirements, Models and Methods (pp. 324–334). Hershey, PA, USA: IGI Global.

Stantchev, V., & Tamm, G. (2012). Reducing Information Asymmetry in Cloud Marketplaces. *International Journal of Human Capital and Information Technology Professionals (IJHCITP)*, *3*(4), 1–10.

Stradistics MRC. (2016). Cloud Computing - Global Market Outlook (2015-2022). Retrieved September 30, 2016, from http://www.strategymrc.com/report/cloud-computing-market

Straub, D. W. (1989). Validating Instruments in MIS Research. *Management Information Systems Quarterly*, *13*(2), 147–169. https://doi.org/10.2307/248922

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1–11.

Sultan, N. (2013). Knowledge management in the age of cloud computing and Web 2.0: Experiencing the power of disruptive innovations. *International Journal of Information Management*, *33*(1), 160–165. https://doi.org/10.1016/j.ijinfomgt.2012.08.006

Sultan, N. A. (2011). Reaching for the “cloud”: How SMEs can manage. *International Journal of Information Management*, *31*(3), 272–278. https://doi.org/10.1016/j.ijinfomgt.2010.08.001

Sundararajan, S., Bhasi, M., & Pramod, K. V. (2017). Managing Software Risks in Maintenance Projects, from a Vendor Perspective: A Case Study in Global

Software Development. *International Journal of Information Technology Project Management (IJITPM)*, *8*(1), 35–54. https://doi.org/10.4018/IJITPM.2017010103

Sutton, S. G., & Arnold, V. (2013). Focus group methods: Using interactive and nominal groups to explore emerging technology-driven phenomena in accounting and information systems. *International Journal of Accounting Information Systems*, *14*(2), 81–88. https://doi.org/10.1016/j.accinf.2011.10.001

Svendsen, G. B., Johnsen, J.-A. K., Almås-Sørensen, L., & Vittersø, J. (2013). Personality and technology acceptance: the influence of personality factors on the core constructs of the Technology Acceptance Model. *Behaviour & Information Technology*, *32*(4), 323–334. https://doi.org/10.1080/0144929X.2011.553740

Tan, W.-G., Cater-Steel, A., & Toleman, M. (2009). Implementing it Service Management: A Case Study Focussing on Critical Success Factors. *Journal of Computer Information Systems*, *50*(2), 1–12. https://doi.org/10.1080/08874417.2009.11645379

Taylor, S., Lacy, S., & Macfarlane, I. (2011). ITIL Version 3 Service Transition. *The Office of Government Commerce*.

Tiemeyer. (2009). *Handbuch IT-Management Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis*. München: Hanser.

Tiwana, A., & Kim, S. K. (2015). Discriminating IT Governance. *Information Systems Research*, *26*(4), 656–674. https://doi.org/10.1287/isre.2015.0591

Todnem By, R. (2005). Organisational change management: A critical review. *Journal of Change Management*, *5*(4), 369–380.

Toval, A., Nicolás, J., Moros, B., & García, F. (2002). Requirements reuse for improving information systems security: a practitioner's approach. *Requirements Engineering*, *6*(4), 205–219.

Trompenaars, F., & Hampden-Turner, C. (2012). *Riding the waves of culture: Understanding diversity in business. rev. and updated*. Nicholas Brealey Publ., London.

Tsai, W.-H., Chou, Y.-W., Leu, J.-D., Chen, D. C., & Tsaur, T.-S. (2015). Investigation of the mediating effects of IT governance-value delivery on service quality and ERP performance. *Enterprise Information Systems*, *9*(2), 139–160. https://doi.org/10.1080/17517575.2013.804952

Turing, A. M. (2009). Computing machinery and intelligence. In *Parsing the Turing Test* (pp. 23–65). Springer.

Valacich, J. S., Schneider, C., & Jessup, L. M. (2014). *Information systems today: managing in the digital world*. Pearson.

Van Bon, J. (2008). *Foundations of IT service management based on ITIL V3*. Van Haren.

Van Bon, J., De Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., & Verheijen, T. (2010). *ITIL®* (Vol. 3). Van Haren.

van de Weerd, I., Mangula, I. S., & Brinkkemper, S. (2016). Adoption of software as a service in Indonesia: Examining the influence of organizational factors.

Information & Management, *53*(7), 915–928. https://doi.org/10.1016/j.im.2016.05.008

Van Grembergen, W., & De Haes, S. (2009). *Enterprise governance of information technology: achieving strategic alignment and value*. Springer.

Van Heijenoort, J., Frege, G., & Gödel, K. (1970). *Frege and Gödel: Two fundamental texts in mathematical logic*. Harvard University Press.

Venkatesh, V., Brown, S., & Bala, H. (2013). Bridging the Qualitative–Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems. *Management Information Systems Quarterly*, *37*(1), 21–54.

Wagner, H.-T., Beimborn, D., & Weitzel, T. (2014). How Social Capital Among Information Technology and Business Units Drives Operational Alignment and IT Business Value. *Journal of Management Information Systems*, *31*(1), 241–272. https://doi.org/10.2753/MIS0742-1222310110

Wallace, L. G., & Sheetz, S. D. (2014). The adoption of software measures: A technology acceptance model (TAM) perspective. *Information & Management*, *51*(2), 249–259. https://doi.org/10.1016/j.im.2013.12.003

Walterbusch, M., Martens, B., & Teuteberg, F. (2015). A Decision Model for the Evaluation and Selection of Cloud Computing Services: A First Step Towards a More Sustainable Perspective. *International Journal of Information Technology & Decision Making*, *14*(2), 253–285. https://doi.org/10.1142/S0219622015500054

Wang, B., Zheng, Y., Lou, W., & Hou, Y. T. (2015). DDoS attack protection in the era of cloud computing and Software-Defined Networking. *Computer Networks*, *81*, 308–319. https://doi.org/10.1016/j.comnet.2015.02.026

Wei, Y., & Blake, M. B. (2010). Service-oriented computing and cloud computing: Challenges and opportunities. *IEEE Internet Computing*, *14*(6), 72–75.

Wester, K. L. (2011). Publishing Ethical Research: A Step-by-Step Overview. *Journal of Counseling & Development*, *89*(3), 301–307. https://doi.org/10.1002/j.1556-6678.2011.tb00093.x

Wheeler, B. C. (2002). NEBIC: a dynamic capabilities theory for assessing net-enablement. *Information Systems Research*, *13*(2), 125–146.

Wiedenhöft, G., Luciano, E., & Testa, M. (2015). Definition of a Model for Measuring the Effectiveness of Information Technology Governance: a Study of the Moderator Effect of Organizational Culture Variables. *CONF-IRM 2015 Proceedings*. Retrieved from http://aisel.aisnet.org/confirm2015/2

Wilkin, C. L., & Campbell, J. (2010). Corporate Governance of IT: A Case Study in An Australian Government Department. *PACIS 2010 Proceedings*. Retrieved from http://aisel.aisnet.org/pacis2010/75

Wilkin, C. L., Campbell, J., & Moore, S. (2013). Creating value through governing IT deployment in a public/private-sector inter-organisational context: a human agency perspective. *European Journal of Information Systems*, *22*(5), 498–511. https://doi.org/10.1057/ejis.2012.21

Worrell, J. L., Di Gangi, P. M., & Bush, A. A. (2013). Exploring the use of the Delphi method in accounting information systems research. *International Journal of*

Accounting Information Systems, *14*(3), 193–208. https://doi.org/10.1016/j.accinf.2012.03.003

Wu, S. S. (2007). Guide to HIPAA Security and the Law. American Bar Association.

Xue, Y., Liang, H., & Wu, L. (2010). Punishment, Justice, and Compliance in Mandatory IT Settings. *Information Systems Research*, *22*(2), 400–414. https://doi.org/10.1287/isre.1090.0266

Yamakawa, P., Obregón-Noriega, C., Novoa Linares, A., & Vega Ramírez, W. (2012). Improving ITIL compliance using change management practices: a finance sector case study. *Business Process Management Journal*, *18*(6), 1020–1035. https://doi.org/10.1108/14637151211283393

Yaokumah, W., Brown, S., & Adjei, P. O.-M. (2015). Information Technology Governance Barriers, Drivers, IT/Business Alignment, and Maturity in Ghanaian Universities. *International Journal of Information Systems in the Service Sector (IJISSS)*, *7*(4), 66–83. https://doi.org/10.4018/IJISSS.2015100104

Yayla, A. A., & Hu, Q. (2011). The impact of IT-business strategic alignment on firm performance in a developing country setting: exploring moderating roles of environmental uncertainty and strategic orientation. *European Journal of Information Systems*, *21*(4), 373–387. https://doi.org/10.1057/ejis.2011.52

Yazdanmehr, A., & Wang, J. (n.d.). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*. https://doi.org/10.1016/j.dss.2016.09.009

Yimam, D., & Fernandez, E. B. (2016). A survey of compliance issues in cloud computing. *Journal of Internet Services and Applications*, *7*(1), 5. https://doi.org/10.1186/s13174-016-0046-8

Yongsiriwit, K., Assy, N., & Gaaloul, W. (2016). A semantic framework for configurable business process as a service in the cloud. *Journal of Network and Computer Applications*, *59*, 168–184.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications*, *1*(1), 7–18.

Zhang, X., de Pablos, P. O., & Xu, Q. (2014). Culture effects on the knowledge sharing in multi-national virtual classes: A mixed method. *Computers in Human Behavior*, *31*, 491–498. https://doi.org/10.1016/j.chb.2013.04.021

[i] https://cloudsecurityalliance.org/research/ccm/