# Implementing cloud services in large french organizations : beyond their IT governance ?

Sabine Khalil

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY

TELECOM ParisTech

2017-ENST-0064

EDITE ED 130

# Doctorat ParisTech

# T H È S E

**pour obtenir le grade de docteur délivré par**

# Télécom ParisTech

## Spécialité “ Sciences de Gestion ”

*présentée et soutenue publiquement par*

**Sabine KHALIL**

24 Novembre 2017

# La mise en œuvre des solutions cloud dans les grandes entreprises françaises : au-delà de la gouvernance des TIC ?

Directeur de thèse : **Valérie FERNANDEZ**

**Jury**

| | |
|---|---|
| **Mme Bénédicte GEFFROY**, Professeur, Sciences de Gestion, Ecole des Mines de Nantes | Rapporteur |
| **M. Sébastien TRAN**, Professeur, Sciences de Gestion, Ecole de Management Léonard de Vinci | Rapporteur |
| **Mme Johanna Habib**, Professeur, Sciences de Gestion, Université de Valenciennes (IAE) | Examinateur |
| **M. Thomas Houy,** Maître de conférences, Sciences de Gestion, Télécom Paristech | Examinateur |
| **Mme Valérie FERNANDEZ**, Professeur, Sciences de Gestion, Télécom Paristech | Directeur |

T H È S E

**Télécom ParisTech**

**école de l’Institut Mines Télécom – membre de ParisTech**

46, rue Barrault – 75634 Paris Cedex 13 – Tél. + 33 (0)1 45 81 77 77 – www.telecom-paristech.fr

# La mise en œuvre des solutions cloud dans les grandes entreprises françaises : au-delà de la gouvernance des TIC ?

**RESUME :** L'avènement de l'internet a entraîné des changements majeurs dans les entreprises ces dernières décennies. De nouveaux modèles d'affaires et services ont émergé affectant les processus métiers et les modes de fonctionnement au sein des entreprises. L'adoption des solutions cloud n'a fait qu'accentuer ces transformations. Si ces solutions ont permis d'améliorer l'automatisation des processus, d'accroître l'agilité organisationnelle, de réduire le time-to-market, et d'assurer des services informatiques à la demande, elles ont également engendré de nouveaux risques pour les entreprises liés à la sécurité, la fiabilité des services, et même la nécessité de nouvelles compétences spécifiques. Comme pour la gouvernance des TIC, les entreprises doivent gouverner leurs solutions cloud afin d'en tirer le maximum davantage et de réduire les risques associés. Bien que de nombreux travaux se soient intéressés à la gouvernance des TIC, peu se sont penchés sur la manière dont les entreprises gouvernent leurs solutions cloud. A cet effet, nous avons décidé de mener une étude qualitative, basés sur la conduite d'entretiens, auprès de 35 grandes entreprises françaises ayant adopté des solutions cloud. Cette étude nous a permis d'explorer les modèles de gouvernance déployés dans les entreprises françaises et d'identifier les liens éventuels entre le modèle de gouvernance déployé et les niveaux d'intensité d'adoption des solutions cloud. Ce travail de thèse met en évidence les différents impacts liés à l'adoption du cloud et souligne l'émergence de plusieurs modèles de gouvernance au sein des entreprises interrogées. Cependant différents facteurs de contingence semblent influencer ces modèles de gouvernance.

**Mots clés :** Solutions Cloud, Systèmes d'Information, Technologies de l'Information et de Communication, Gouvernance, Transformation Digitale, Grandes Entreprises.

**Implementing Cloud Services in Large French Organizations: Beyond their IT Governance?**

**ABSTRACT:** Throughout the last decades, the Internet has brought a myriad of innovative services in organizations. Cloud computing has been a part of Information Technologies that have transformed organizations. It enhances automation and agility, allows scalability and ubiquity as well as reduces time-to-market. However, previous research studies in the IT field has taught us that organizations cannot sustain in a competitive market without, first, investing in IT, and then, effectively governing it. For instance, the extensive list of failing organizations, due to their bad IT governance, has raised awareness regarding the importance held for effective governance. Therefore, organizations can use their investments in IT to their benefits when governed effectively. Similarly, in order to reduce risks generated when adopting cloud services, and benefit from the promised advantages, organizations should effectively govern them. Nevertheless, to our knowledge, no cloud governance model, addressing the various angles of cloud computing, exists. While this research work is motivated by the primordial need for governance, it explores cloud governance adopted by large French organizations, and whether it can be achieved through the organizations' IT governance. In addition, it aims at studying the possible link between the organization's effective cloud governance and the intensity level of their adoption. We conduct 35 interviews with large French organizations that have adopted cloud services in order to meet the objectives of this research work. The two rounds of interviews with the 35 organizations highlight numerous major impacts of cloud computing. From the results arise different possible governance models when adopting cloud services in large organizations, along with various factors affecting this governance. We finally stress on the originality of our contributions in the IT and cloud governance literature, as well as we draw the light on the impact of theoretical and practical implications to the Information Systems community.

**Keywords**: Cloud Computing, Information Systems, Information Technology, Governance, Digital Transformation, Large Organizations.

TELECOM ParisTech

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY

# Acknowledgment

With great honor and privilege, I would like to express my sincere appreciation to several particular individuals who were largely influential in the completion of my PhD.

I would like to start by thanking my supervisor Prof. Valérie Fernandez, for whom I have enormous respect and to whom I owe an inestimable debt of gratitude. You were more than a mentor to me. Thank you for coaching me, guiding me, and engaging with my ideas throughout the different phases of this dissertation. Valérie, you were there whenever I needed support, or guidance. You taught me to manage my time, become more independent and more efficient. Thank you also for being such a great leader as the head of our department. Your positive energy and presence appease the entire Economics and Social Sciences department. I was lucky to have you as my supervisor – I know many would wish to be one of your PhD students. Thank you Valérie!!

I would also like to express my gratitude to the members of my jury who accepted to evaluate this research work. I am truly grateful to have honorable professors guiding through my thesis dissertation. I would like to thank Prof. Bénédicte Geffroy and Prof. Sébastien Tran for their constructive comments, rich advice and valuable reports. I would also like to thank Prof. Johanna Habib and Thomas Houy for the time and effort they will invest examining my doctoral work.

I would also like to thank Prof. Till Winkler from Copenhagen Business School, who took interest in my doctoral research. Thank you for the fruitful collaboration in Copenhagen, the challenging subjects and the numerous opportunities. I wholeheartedly appreciate your advice, constructive comments, and guidance. Thank you for sharing your expertise and knowledge with me. You have shown me multiple successful ways to address my research question. Through our collaboration, I also had the opportunity to meet brilliant researchers from the Digitalization Department of CBS. And of course, thank you for that wonderful home-made meal with your lovely family. I sincerely enjoyed the random discussions with you and Luna.

Prof. Maksim Belitski, from the University of Reading! From where do I start? Thank you for showing interest in my research subject. You have taught me how to always find a solution for any challenge faced in the academic world. Thank you for pushing me towards the quantitative analysis. Collaborating with you was highly enriching, whether it was at the University of Reading, after playing a game of chess at Henley Business School, through sharing inspirational moments during our walks along the Thames River, during our long car drives, or even over a burger at le 'Marais Chic'. Your fun spirit has truly brought sun rays to gloomy England.

I would like to also thank the "*Fondation Nationale pour l'Enseignement de la Gestion des Entreprises"* (FNEGE) for selecting me to be part of the program entitled "*Centre Européen de Formation Approfondie à la Gestion*" (CEFAG). I was lucky to be part of this program as it increased my research expertise in the academic world, through two seminars offered by some of the best business professors in France. I would like to thank them for the time and advice they offered us. Through these seminars, I had the chance to meet brilliant PhD students, with whom I shared deep conversations, serious discussions, and many fun times. The CEFAG also provided me with the opportunity to go to a business school of my choice, as a visiting researcher. I show my deepest gratitude to the FNEGE for this amazing experience.

Who’s next? I think the time has come to thank you. You’ve never let me down. You’ve always been by my side to never feel alone, behind my back to support me, and in front of me to help me face any challenge in my life. You are my mentor, you are my idol, and you are my greatest inspiration. Carine Khalil, a.k.a. my sister, thank you for everything. I don’t even know from where to start – I know we should keep the acknowledgements section short, but I can’t help it. I don’t know why I was so lucky to have you as my sister. You’ve always been there for me, you’ve helped me so much, and you’ve made me feel better so many times. You’ve taught me how to be strong, how to be happy, and most importantly how to survive a PhD. Thank you, thank you, and a thousand times thank you. I don’t think I would’ve made it this far without you in my life. *inserts monkey emoji*

My lovely family (Antoine, Miranda and Khalil – since Carine got her own private paragraph – Although I guess she deserved it for putting up with me, especially during the last 3 years). My wonderful loving, cute, little family! Thank you for your support. Thank you for your encouragement. Thank you for being there for me. I don’t think I would be writing my PhD acknowledgements today if it weren’t for your continuous support. Thank you for your unconditional love, your amazing care, and your encouraging words. I love you from the bottom of my heart. *inserts heart emoji*

My Parisian family! Here comes the time to thank you guys! You all know yourselves. I know I’ve been babbling for a while now, so I will try to keep it short (I apologize for not being able to thank each and every one of you individually). You earned yourself the title of my bestfriend. Even in such a short amount of time, you’ve totally earned it Mook. I want to start by thanking you for putting up with me and my fluctuating mood during my PhD. Your loving words, your positive vibes, and your uplifting messages helped me survive it. You know why? Cause we started from the bottom now we here (sorry can’t really continue the song). Thank you for always being there for me, no matter what. Thank you for being in my life Mook, love YA!!! Coloca, gracias por todo! Gracias por los ‘post-it’, por tus palabras de aliento, por tu apoyo diario, por la energia Colombiana muy positiva en nuestro cuarto, por las arepas deliciosas, y por tu amor. Te quiero mucho (ah y quiero agradecerte por todas las historias ‘glauques’ antes de dormir). Habibi Fatayer, merci pour tout ton soutient et ton amour. Merci d’avoir passé la majorité de mes pauses avec moi, et surtout, d’avoir partagé les moments Ben n Jerry’s/Fatayer/Ciné. Je ne vais surement pas oublier de te remercier pour tous les spectacles et toutes les danses privées auxquelles j’ai eu droit. Marou Marou Tahiti ! (Je voulais te dire je t’aime en tahitien mais j’ai oublié les mots et j’ai la flemme de traduire sur google.. Bref, je t’aime). Zaidab, je veux surtout de remercier pour TOUS tes câlins et tes bisous. Tous ces clichés sur les russes sont totalement faux, tellement j’ai eu droit à des câlins. Merci pour ton soutient Zaidab !! *je t’aime en russe*. Merci à toute ma famille parisienne et mes collègues à Télécom Paristech et je m’excuse pour tous les ‘*désolée je ne peux pas, je dois bosser ma thèse’* que j’ai sorti durant ces 3 ans !

A final thank you note goes to my talented physical therapist Claire Robquin, without whom I would have never been able to sit in front of my laptop for 12 hours a day.

# Table of Contents

# List of Figures

# List of Tables

# List of Abbreviations

| | |
|---|---|
| **Amazon EBS** | Amazon Elastic Block Store |
| **AUP** | Acceptable Use Policy |
| **AWS** | Amazon Web Service |
| **CAPEX** | Capital Expenditure |
| **CDO** | Chief Digital Officer |
| **CEO** | Chief Executive Officer |
| **CIO** | Chief Information Officer |
| **CMM** | Capability Maturity Model |
| **CMM1** | Level 1 of Cloud Maturity Model by the ODCA |
| **CMM2** | Level 2 of Cloud Maturity Model by the ODCA |
| **CMM3** | Level 3 of Cloud Maturity Model by the ODCA |
| **CMM4** | Level 4 of Cloud Maturity Model by the ODCA |
| **CMM5** | Level 5 of Cloud Maturity Model by the ODCA |
| **CMMI** | Capability Maturity Model Integration |
| **CNIL** | Commission Nationale de l'Informatique et des Libertés |
| **COBIT** | Control Objectives for Information and related Technology |
| **CSN** | Cloud Service Partner |
| **CSP** | Cloud Service Provider |
| **CSU** | Cloud Service User |
| **DCR** | Decision Control Rights |
| **DMR** | Decision Management Rights |
| **EC2** | Elastic Compute Cloud |
| **HR** | Human Resources |

| | |
|---|---|
| **IaaS** | Infrastructure as a Service |
| **ICT** | Information and Communication Technologies |
| **IEC** | International Electrotechnical Commission |
| **IoT** | Internet of Things |
| **IS** | Information Systems |
| **ISO** | International Organization for Standardization |
| **IT** | Information Technology |
| **ITBSC** | IT Balanced Scorecard |
| **ITGBSC** | IT Governance Balanced Scorecard |
| **IT-CMF** | IT-Capability Maturity Framework |
| **ITCI** | Information Technology Governance Institute |
| **ITIL** | Information Technology Infrastructure Library |
| **KPI** | Key Performance Indicators |
| **NIST** | National Institute of Standards and Technology |
| **NSA** | National Security Agency |
| **ODCA** | Open Data Center Alliance |
| **OPEX** | Operational Expenditure |
| **PaaS** | Platform as a Service |
| **PP** | Private Policy |
| **S3** | Simple Storage Service |
| **SaaS** | Software as a Service |
| **SAM** | Strategic Alignment Model |
| **SLA** | Service Level Agreement |
| **SMEs** | Small and Medium Enterprises |
| **ToS** | Term of Service |

# Introduction

*The sun always shines above the clouds – Paul F. Davis*

This chapter provides readers with a background on Information Technology and Cloud Computing. It starts by introducing the fast technological shift witnessed in today's society and fast-growing market. It then presents the emergence of new technologies, such as cloud services, and the reasons behind their widespread adoption across most organizations today. The author emphasizes the critical role governance plays in the sustainability of organizations. In addition, the research question, the aims and the objectives of this work are explained in this chapter. Finally, the author ends with a description of the thesis structure while giving a brief summary of every chapter.

# I. The Road to Effective IT Governance

'Avoir la tête dans les nuages' is a common French expression that literally translates to 'having our minds in the clouds'. When one 'has their mind in the clouds', it means they are distracted, or they are disconnected from reality. With the help of the Internet, it is extremely easy today to be disconnected from reality and instead be connected to virtual reality. Virtual reality, as contradictory as this may sound, represents our society today; people located in France are playing virtual soccer with others located in the USA through a virtual platform, a teacher in Denmark is giving virtual classes to their students in the UK through video recordings, a mother at work is virtually checking up on her children at the daycare through her smartphone. Endless examples illustrate the way our society today is changing from a reality in which human beings live, to a virtual reality created by new technologies and made accessible through the Internet.

Throughout the last decades, the Internet has brought a myriad of innovative services for those who are connected to virtual reality. From the long list of transformations impacting society, the Internet has been reshaping radio, telephony, television, paper mail, and newspapers, for example. These traditional methods of communication and media have been redefined by the Internet into new services; music streaming, video calls, Internet telephony, Internet television, emails, and digital newspapers. A large number of traditional services have been reshaped into digital services that are accessible via the Internet. Several communication media services are now adapting a website technology to keep up with the digitalized society. Along with digitalized communication, personal interactions have increased through the creation of social networks, instant messaging, and virtual forums. The emergence of the digital wave has revolutionized society. When a son, living abroad, needed to ensure his parents about his well-being, his paper mail took months before arriving to its destination. However, today, a simple message on his smartphone reaches his parents in just fractions of a second. The digital era has not only accelerated communication, but has also made them easier. With a simple click a person can buy gifts online, check their bank account, monitor their health status, reserve accommodation, or even get the road itinerary. All these new services are achieved through the emergence of new technologies that are used via the

Internet. Emerging technologies represent contemporary innovations in different fields of technology[1], such as nanotechnology, biotechnology, cognitive science, educational technology and Information Technology. In this research work, we are going to focus on Information Technology (IT) as it is playing a major role in organizations' activities and strategies.

IT represents the ensemble of computers and networks along with the different tools and expertise implemented by organizations in order to generate, process and distribute information throughout the organization (Chandler and Munday, 2012). IT has been part of the organization's Information System (IS) for several decades while providing numerous benefits. Many researchers argue that IT plays a highly important role in achieving business value (Henderson and Venkatraman, 1999; Sambamurthy and Zmud, 2000; Reich and Benbasat, 2000; Weill and Ross, 2004; Brown and Grant, 2005). It is also regarded as an indispensable tool for improving the organization's competitive advantage (Oliveira and Martins, 2011) through enhancing the organization's inventory management, and improving its customer services (Tallon et al., 2000). In the last decade, the role of IT in organizations has been evolving from its traditional back-office to a more strategic role, influencing business strategies (Tallon et al., 2000). Therefore, Information Technology has become an integral part of businesses, providing organizations with a significant competitive advantage.

For the last two decades, a large amount of money has been spent in IT investments. The Canadian government reported a total of 8.7 billion in Canadian dollars for IT projects between 2003 and 2006 (OAG, 2006). In addition, the US government also reported a total of 80 billion dollars of annual investments in IT (Pang, 2014). While a growing number of organizations rely on IT in today's competitive market, IT development, implementation and management remain a challenge for many of these organizations. The number of successful IT projects, delivered on time and within budget, is still considerably low according to many international surveys (Standish Group, 2015; VersionOne, 2016). The lack of management involvement and communication, the poor requirement specifications and objectives definition, the lack of project management skills and methodologies, as well as the non-alignment to organizational needs and strategies among the common factors that explain the

[1] http://conferences.oreillynet.com/pub/w/18/keynotes.html

failure of IT projects (Schmitt and Kozar, 1978; Bussen and Myers, 1997; Taylor, 2000; Humphrey, 2005; Standing et al., 2006; Standish Group, 2015).

A large amount of research studies in information systems and project management have addressed the challenges associated with the development, adoption and use of IT in organizations. While a number of studies in the IS field has focused on the way these technologies are managed, others stress on the way these technologies are governed.

We witnessed through the last two decades the emergence and adoption of innovative project management methodologies so-called agile methodologies. Unlike traditional methodologies, these value iterative development, close collaboration between the client and the development team as well as constant adaptation to changes. According to many research studies, agile methodologies help address the problems related to the lack of user involvement, executive management support, as well as clear statement of requirements (Standish Group, 2015). Beyond these challenges associated with the development and the management of IT, IT projects can fail because of a lack of governance. In fact, IT management can be considered a part of IT governance. While IT management focuses on managing the present IT services and IT operations, IT governance contributes to the present business operations and positioning IT in order to meet future demands. In addition, IT management emphasizes the organization's internal side (business focus), where IT governance goes further and focuses on its internal and external sides (business customers focus) (Van Grembergen et al., 2004; Peterson, 2004).

Before going any further, let's start by defining the word 'governance'. Governance is a common term deriving from a Greek verb that means 'to steer'. The term governance is usually used in politics referring to the activity of ruling a country (hence the reference to the word 'government'). Following this usage, organizations have started to adopt governance as a mean to steer their departments, in order for them to interact and keep the organization under control. In fact, governance in an organization consists of developing a long-term strategy, while installing policies for employees, to follow a specific organizational behavior. Governing the organization generates a myriad of benefits such as satisfying the expectations, improving the organization's performance and cultivating its economic growth (Weill, 2004). Through the presence of easily-adopted policies and the facilitated communication throughout the organization, governance is beneficial (Taylor, 2000; Humphrey, 2005; Standing et al., 2006). This leads to better decisions that are more fitting to the organization's mission and to the creation of more synergies and communication between departments. In addition, organizational governance restores control while minimizing corruption, risks, and mismanagement. For instance, when employees know which policies they need to follow, what they are required to do and how they need to do it, organizations notice lower risks and lower mismanagement (Damianides, 2005).

With the increasing importance of IT in organizations, the need for governing IT has progressively risen. Additionally, many internal and external pressures – as explained infra – have strengthened this urge for governing IT. First, the fast growing market has led to more competitiveness and a lower time-to-market for organizations, pushing them to have a better strategic alignment between their IT and business departments (Bharadwaj et al., 2009). Moreover, with the increasing amount of money spent on IT, organizations need a more cautious control of the return on their IT investments. Furthermore, organizations increased their focus on corporate control and requirements due to the appearance of the Sarbanes-Oxley act[2]. Such acts require a higher transparency and accountability regarding IT investments. Based on these internal and external pressures, IT governance seems primordial for the correct, transparent, and consistent behavior of organizations.

Regarding IT governance, numerous definitions exist in the literature. While some researchers state that IT governance consists of allocating the different decision-making loci for rights and accountabilities (Weill and Woodham, 2002; Simonson and Johnson, 2006), others state that it focuses on adopting mechanisms to achieve the organization's strategy (Korac-Kakabadse and Kakabadse, 2001; Van Grembergen and De Haes, 2009). However, additional research works affirm that IT governance is responsible for the allocation of decision rights as well as the adoption of governance mechanisms to deploy these decisions (Luftman and Brier, 1999; Sambamurthy and Zmud, 2000; Peterson, 2004; Weill, 2004). This last definition regroups the first two definitions presented, and hence it addresses different aspects of IT governance. We, thus, decided to base our research work on it, in order to get a holistic vision of IT governance and tackle it from the various angles.

---

[2] A mandatory act forcing every organization to comply to the various mentioned regulations (http://www.soxlaw.com/index.htm)

Governing IT is not an easy task. According to the London School of Economics study conducted in 1998, only 25% of 659 CEOs expressed their satisfaction with the performance of their organization's IT investments (CSC Index, 1998). This low level of satisfaction can be explained by unmet demands, long time-to-market, and power solely allocated to the IT department. Despite the implementation of IT governance, several organizations still face serious cases of IT failures. According to the Standish Group, while 44% of IT investments were challenged in 2010, 24% failed (Standish Group, 2010). The following key factors have been identified in the literature as impacting IT governance: (1) taking relevant IT decisions, (2) allocating these decisions to the appropriate decision makers, and (3) implementing key mechanisms that facilitate the effective adoption of IT governance. First, (1) managers discuss the different decisions to be made regarding their IT, such as the budget allocated to purchasing equipment, the policies to implement, the need to internally develop services or to outsource them, etc. Then, (2) the lack of alignment between IT and business executives seems to increase the latter's' skepticism regarding IT benefits. Thus, integrating business executives' opinions in the decisions related to IT investments helps the business strategy in gaining more support from IT. Some researchers argue that the levels of importance CEOs allocate to IT along with their perceptions are linked to the organization's IT implementation levels (Jarvenpaa and Ives, 1991). While business and IT executives may have different objectives and different interests, it is imperative to align these objectives through effectively governing IT. Organizations have accepted IT as a strategic asset supporting their overall strategy and pushing them forward, which highlights the primordial role IT governance plays in organizations. Therefore, allocating IT-related decisions to the appropriate decision makers is a key factor when implementing IT governance. Finally, (3) when IT-related decisions are allocated to the appropriate decision makers, implementing governance mechanisms (such as decision-making structures, business processes, and relational mechanisms) supports the alignment between IT and business departments, and allows an effective adoption of IT governance.

As mentioned in IT governance related-work, these key factors should be taken into consideration. Previous studies show that investing in IT can become harmful for the organization when (1) the right decisions are not taken and/or when (2) the decision makers are not responsible for the appropriate decisions, and/or when (3) no governance mechanisms have been implemented (Weill and Ross, 2004; Van Grembergen et al., 2004). It is therefore imperative to adopt effective IT governance (and hence, the three previously mentioned factors) in order to benefit from the numerous advantages generated by IT. We will address these factors in detail in Chapter 2.

The following facts illustrate a few examples of failures when IT governance was not implemented effectively. While poor investment decisions led to a cancelation of 11 billion British pounds at the British National Patient System (Hough, 2011), IT assets failed to process tickets during the 2008 Olympics in Beijing ("Olympics Ticket Sales", 2007). Moreover, IT security breaches have been present since the evolution of the Internet, affecting well-known organizations such as Linked-in, Google, Apple, Facebook, TJX, etc. A recent cyberattack hit more than 10 countries, including France, the United Kingdom, Spain, Australia, and Russia, and pushed the French organization Renault to close several factories and become extra vigilant with their IT ("Renault Touché par la Cyberattaque", 2017). Therefore, in order to avoid such catastrophic incidents, organizations are advised to understand the meaning of effective IT governance, instead of adopting it blindly. Effective IT governance for us represents the adoption of governance mechanisms that are fully immersed in the decision-making process and entirely in line with the desired outcomes of stakeholders and decision-makers. The main objective of adopting governance mechanisms is to support the decisions made and facilitate their implementation. Furthermore, the emergence of new technologies today is exposing organizations to higher threats and a larger possibility of outsider attacks. Therefore, due to the high amount of cyberattacks, security breaches and massive investments made in IT, effective IT governance is primordial.

## II. The Road to Effectively Governing Cloud Computing

Organizations have witnessed the emergence of numerous new technologies. Cloud computing, for instance, is a new technology that appeared in the beginning of the 21st century and has been a part of the revolution of today's society. Cloud Computing can be traced back to utility computing, a concept promoted by Carr (2003, 2005). Along with the title of his highly read articles, Carr (2003) claims that the traditional corporate computing is coming to an end; it will be replaced by a simple utility model. He states, "*As information technology's power and ubiquity have grown, its strategic importance has diminished. The way you approach IT investment and management will need to change dramatically*" (2003, p. 41), and continues "*After pouring millions of dollars into in-house data centers, companies* *may soon find that it's time to start shutting them down. IT is shifting from being an asset companies own to a service they purchase*" (2005, p. 67). These statements highlight the changes affecting organizations when dealing with IT and their need to shift towards cloud services. Several researchers emphasize the transformations brought when implementing cloud technology; for example, challenging the organization's traditional IT governance approaches, managing its IT landscape, adjusting its processes (Yanosky and Caruso, 2008; Armbrust et al., 2010; Winkler and Brown, 2014; Ragowsky et al., 2014; Schneider and Sunyaev, 2016). In addition to these internal transformations, cloud services have challenged organizations into developing their employees' skills (Rajendran, 2013; Dutta et al., 2013; Oredo and Njihia, 2014). Deploying new services, such as the cloud, requires new capabilities in order to understand the functionality of the adopted services.

Nevertheless, the transformations generated by cloud technology should not be taken for granted as usages are increasing daily. In accordance with a report presented by Ried et al. (2011), the cloud computing market is expected to reach $241 billion in 2020, compared to $40.7 billion in 2010; a 600% increase in a span of 10 years. Cloud services have been gaining popularity due to their large list of benefits. The literature has broadly studied cloud benefits along various categories—the most frequently cited are related to economics (e.g. low costs, pay-per-use, low electrical consumption), scalability (e.g. dynamically scaling resources up and down), agility (e.g. agile processes and lower time-to-market), and ubiquity (e.g. ubiquitous cloud usage) (e.g. Chebrolu, 2011; Rajendran, 2013; Zhang et al., 2010). Adopting cloud services has facilitated tasks for numerous organizations. To illustrate the large set of benefits available to various facets of today's society, The New York Times has been using public cloud solutions provided by Amazon (the Elastic Compute Cloud[3] and the Simple Storage Service[4]) to transform 11 million scanned archived newspapers from the year 1851 till the year 1980, into PDF files available for the public and free of charge. Moreover, according to a survey conducted by Gartner (2015), they forecast an increase in cloud services adoption to $312 billion by 2019, with a yearly growth of 15%. It is important to notice that

[3] Elastic Compute Cloud is a cloud platform service offered by Amazon, allowing users to rent virtual machines on which they can run their own applications.

[4] Simple Storage Service is a cloud web service offered by Amazon, allowing users to store their data through web service interfaces.

the higher the intensity level of cloud services adopted, the more the organization can benefit from the different opportunities. However, adopting cloud services would be '*too good to be true'* if it were risk-free. The literature also identifies most commonly mentioned risks, which are related to security (e.g. insider and outsider attacks, data loss, data confidentiality), compliance (e.g. integrity and regulation laws), and reliability (e.g. downtime, availability of servers, congestion) (e.g. Dutta et al., 2013; Onwubiko, 2010; Srinivasan, 2013). This also leads to the fact that the higher the intensity level of cloud services adopted, the more the organization is faced with risks.

For illustration purposes, the Sky High survey claimed that in 2016, an organization adopts on average 37 file sharing (cloud) services, such as, OneDrive, WeTransfer, Dropbox, Google Drive, etc. First, this large amount of services increases the organization's costs as each service possesses many small licenses, which add up to a larger amount. In addition, collaboration between departments becomes harder when each one uses a different platform to share their files. Moreover, while these services are not always secure, they increase the risks in the organization. It is important to be aware that not every cloud service offered is actually risk-free. For instance, the Sky High survey (2016) identifies the top 10 most approved cloud services: OneDrive, Salesforce, SharePoint Online, Exchange Online, Cisco Webex, Skype for Business, Concur, Box, Oracle Taleo, and ADP. These services vary in functionalities, including file sharing, customer relationship management (CRM), video calls, etc. On the other side, the survey also pinpoints the top 10 most outlawed cloud services; the Pirate Bay, PDF split, PicResize, KickTorrent, PDFUnlock, DocSlide, 4Shared, Pastebin, WebICQ, and PDF to Doc. The functionalities of these services also vary; illegal downloads, splitting PDF files, unlocking PDF files, sharing files, converting PDF files into Microsoft Word files, etc. It is important to identify these services for organizations to become aware of the high risk associated with each cloud service they desire to adopt. However, many employees remain unaware of the high risks engendered by such outlawed services. For instance, some might need to split their PDF files into several documents using the PDF split online service. Had the files possessed sensitive and critical information, the simplest task of splitting them would have been highly dangerous and the files would have been potentially hacked. Organizations must be aware that security controls vary from one cloud service provider to the other, making every cloud service differently secured. Therefore, before the adoption phase, organizations need to ensure the security of the desired services through the contracts signed with their cloud service providers.

As business departments are blindsided by the benefits generated by cloud services, they generally use them without the help of their IT department. Based on the previously illustrated examples, employees think they can safely upload a corporate file to the Internet and use such services, risk-free. Without any expectation, their ignorance and lack of awareness of all possible risks increase the level of threats hitting the organization. Therefore, governing cloud solutions is a critical mission for organizations today, during the fast-growing and overwhelming digital wave. Governing cloud computing is not an easy task to accomplish, due to the diverse transformations it engenders. Many analogies compare the governance of cloud services to several concepts. One interesting analogy is comparing it to a cat, where cloud users think they are in control until the cat decides it's playtime, food time, or simply 'leave me alone, I want to sleep' time. Cloud services are known for being hard to control, where providers have the power to do as they please. This exaggeration illustrates the difficulty that organizations go through when adopting cloud services. Therefore, to avoid such high risks and increase their security level, it is imperative that they control and monitor their departments as long as they are adopting cloud services.

As important as monitoring cloud services seems, the academic literature tackling cloud governance models is still scarce. While only few research works present a governance model for cloud computing, they do not address all of its different angles, and do not present the different steps leading to effective governance of cloud services.

Meanwhile, cloud services are part of the organization's IT. Thus, to simplify the tasks on organizations, it might be possible to govern them through their IT governance. However, due to the diverse transformations engendered by cloud services, and the numerous risks generated, we surmise that an organization's IT governance needs to be adapted to cloud computing. Therefore, the research question of this thesis is: "*Does the adoption of cloud services require a specific governance model?*"

The following sections are devoted to elucidate the research aim and objectives, and then present the thesis structure from the introduction to its conclusion, in order to find answers to the stated research question.

# III. Research Aim and Objectives

This research work is motivated by the primordial need for governance. Several previous cases of ineffective governance emphasized the importance of effectively governing organizations' IT. Based on these numerous incidents, IT governance appears to be critical for the success of organizations. In addition, the emergence of cloud services propagates various transformations within the organization. In spite of the large set of benefits promised by cloud computing, it also generates numerous risks. These engendered risks hamper the adoption of cloud services for organizations. Therefore, in order to increase cloud adoption, the importance of governance is accentuated today.

The objective of this research work is to first explore whether cloud services can simply be governed through the organization's IT governance or if they require specific governance. In the latter case, this research aims at studying the different aspects needed to effectively govern cloud services.

## IV. Thesis Structure

We started the research presented in this thesis with an introduction (Chapter 1). This chapter introduced the rise of IT governance in organizations throughout the last decades. Along with the rise of IT governance, organizations witnessed the emergence of new technologies, such as cloud computing, leading to a large number of transformations for organizations as well as for employees. These transformations prompted organizations to seek different ways to address them, thus highlighting the need to govern cloud services. Therefore, we questioned whether deploying cloud technologies in an organization required a specific governance model.

In order to introduce and explain the context of this thesis (IT governance and the deployment of cloud services by organizations), Chapter 2 is devoted to presenting the literature review under three sections. The first section offers an introduction to Information Technology and its different aspects, with a special focus on IT governance. The following section of the literature review covers the cloud computing concept as an emerging technology, while focusing on the transformations it engenders and the governance models proposed by other researchers. The third section presents the existent maturity models in the literature while emphasizing the benefits generated through assessing the maturity of organizations. Chapter 2 also identifies the different research problems of this thesis that emerged through exploring the Information Systems literature.

The aim of Chapter 3 is to identify and develop the research design of this thesis. It first provides the foundations regarding the methodological approach, the philosophical epistemology, and the research methods used by authors in the IS field. The second part of this chapter explains our choices required to conduct the research presented in this thesis; a qualitative methodological approach, an interpretivist philosophical epistemology, and interviews and documentation as the methods adopted. It then provides the reader with a detailed explanation of these methods, where two rounds of interviews were conducted (Part I and Part II). Finally, the chapter discusses the methods adopted to analyze the two rounds of interviews.

In Chapter 4, we introduce the results from our analysis, which is divided into two parts. The first part (Part I) mainly identifies the need for specific governance when adopting cloud services. While participants mention the various benefits and threats generated by cloud technologies, they also highlight the different transformations engendered by their adoption. The second part (Part II) is devoted to unveil the possible correlation between organizations' IT governance and their intensity level of cloud adoption. This correlation is studied through the application of the Cloud Maturity Model proposed by the Open Data Center Alliance (ODCA, 2013). Based on this model, we calculate the cloud maturity of each interviewed organization. Then, this chapter presents different governance models for organizations showing different cloud adoption intensity levels. An in-depth analysis of this correlation follows.

Chapter 5 displays an overall representation of the results emerging from Part I and Part II, while comparing our findings to the current literature review (Chapter 2). Following this comparison, we outline the contributions regarding the main constructs of this thesis; the need for specific governance when adopting cloud services and its correlation with the intensity level of adoption. We, then, discuss the key limitations of this work and bring out the originality and novelty of our contribution, while providing directions for future research.

The last chapter (Chapter 6) summarizes this work while stating concluding remarks.

Figure 1 represents the detailed outline of this thesis.

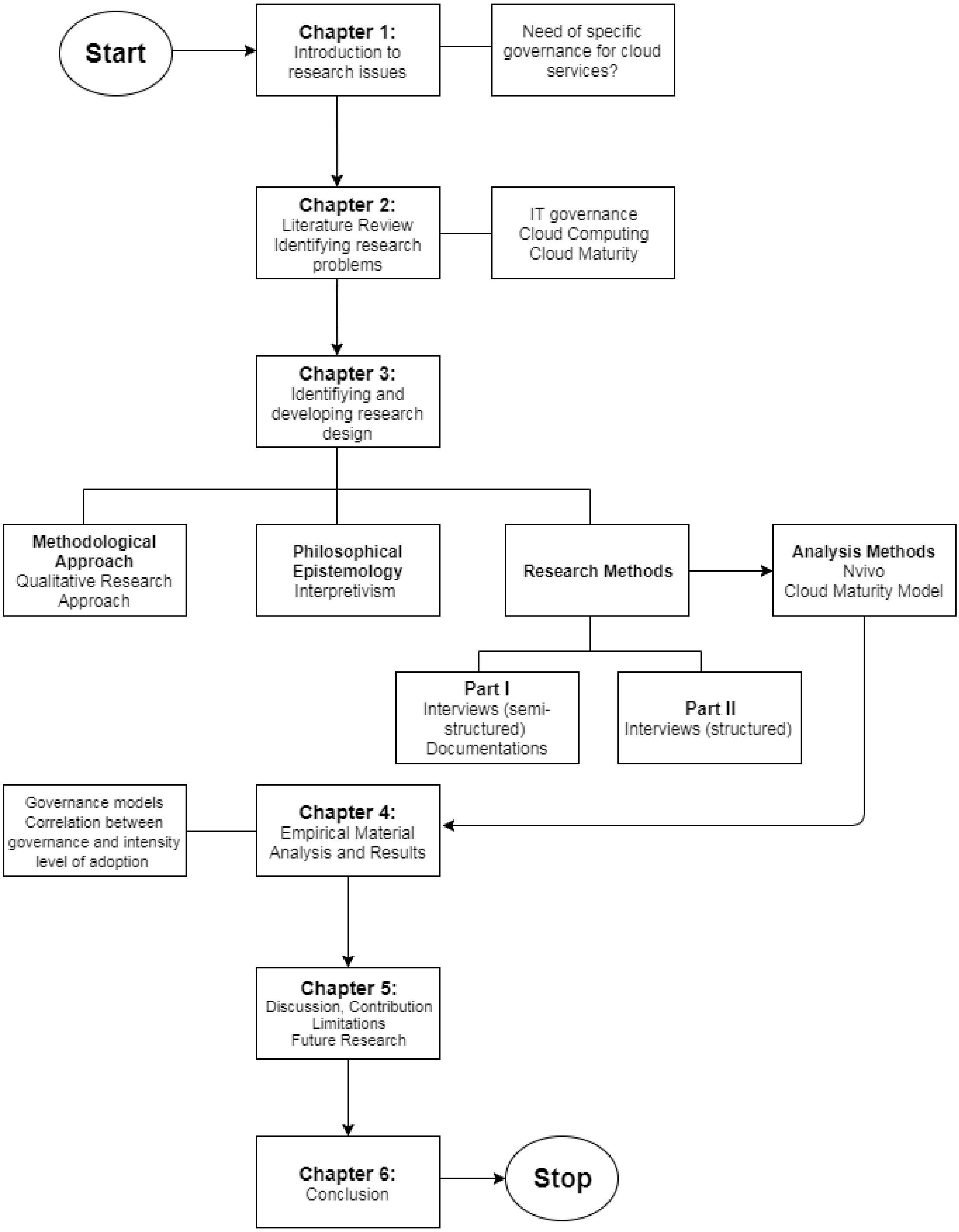


**Figure 1: Thesis structure**

# Literature Review

This chapter represents the literature review on which our research work is based. It aims at reviewing and critically analyzing previous work in the Information Systems area. The chapter is divided into three sections. The first section describes an IT governance background in the Information System domain. The author addresses various subsections regarding governance with a focus on Information Technology; its use, the domains it covers, and the way to govern it. The second section of this literature review offers an overall description of cloud computing. This section introduces the various aspects characterizing cloud services, including their emergence, ecosystem, service and deployment models, benefits and risks, contracts, impacts on organizations, and the existing governance models. Finally, the last section is responsible for reviewing the maturity models studied by previous researchers, with a focus on the cloud maturity model proposed by the Open Data Center Alliance. We conclude this section with a critical analysis of the reviewed research works.

# First Section: IT Governance Background

## I. Information Systems

### 1. What are Information Systems?

The concept of Information Systems (IS) emerged during the 1960s. Since then, most organizations cease to exist without implementing an information system, as it constitutes their backbone. Such systems were allocated several definitions. The simplistic definition of an information system is that it manages and processes information within the organization (Van Der Aalst and Stahl, 2011). As noted by Tran (2012), while Information Systems play a vital role in an organization's investment choices, they are mostly deployed for strategic reasons.

In addition, classifying Information Systems has been popular in the literature (Alter, 2002; Dumas et al., 2005; Olivé, 2007). Three IS classes represent the most general classification in the actual literature; personal IS, public IS, and organizational IS. While personal Information Systems are responsible for managing as well as storing information privately accessible by a person, such as a personal collection, public Information Systems are responsible for managing and storing information publicly accessible by a community. On the other hand, organizational Information Systems support information of an organization. We will rely on the latter Information System class for the rest of this research work.

An organizational Information System consists of numerous resources, including the players (users of the system, internally – employees, executives, managers – and externally – clients, suppliers, etc.) who either use the information or feed the system with new data. A second resource of IS is the data, which constitute vital information for the business operation. Software and hardware are also a part of the IS resources, where computing technologies are required. However, an IS is not only based on resources, but also on individual and collective work practices which constitute the dynamic part of the system. Figure 2 shows the constitution of an organizational Information System. An IS aims at collecting information, analyzing them, and storing them to finally communicate them. It is also a multidimensional system, including, technological dimension (IS founded on an architecture), organizational dimension (IS supporting organizational structures and processes), and informational dimension (IS producing outcomes based on data) (Reix et al., 2016). Moreover, as Reix et al. (2016) emphasize, an Information System is not a ready-to-use resource, instead it represents a system that must be defined and built while integrating the three previously mentioned dimensions (technological, organizational, and informational).

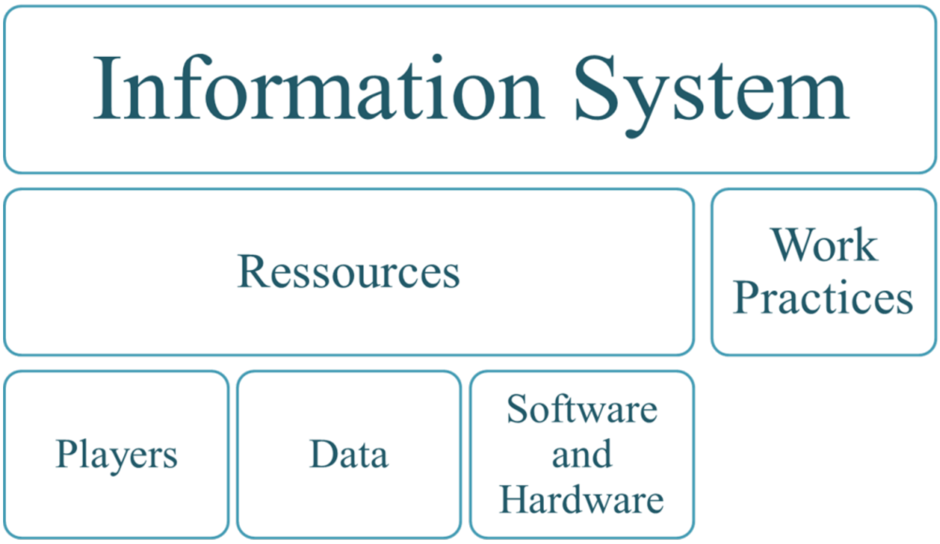


**Figure 2: Elements of an Information System**

## 2. What is Information Technology?

Information Technology (IT) combines computing and telecommunications in order to process and transmit information in different forms (text, voice, or pictures) (Turban et al., 2001). IT refers to "*the study, design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware*[5]". It consists on retrieving, protecting, processing, and converting information via the use of software and electronics. IT professionals are responsible for designing complex computer networks, managing and designing databases, as well as managing and administrating the entire systems (Sharma, 2012). IT consists of work practices as well as several resources similar to the ones composing the IS; IT is also composed of data, software and hardware. However, unlike IT where all the systems are computer-based, IS can be formed of several tools brought together to create a system that records information. In addition, IS have existed before the mechanical era (for example, in the form of books) where

[5] https://www.igi-global.com/dictionary/information-technology/14539

IT has emerged with the creation of computers. Figure 3 represents the major components of Information Technology in an organization.


**Figure 3: Elements of Information Technology**

## 3. Why is IT Important for Organizations?

Information Technology has been playing an important role in organizations. For instance, the number of organizations, today, depending on IT to reach their business needs is seen to be increasing. In today's dynamic and unstable markets, IT has become primordial and pervasive, forming an integral part of businesses. Several authors agreed on the positive link between using IT in an organization and its increased performance (Broadbent and Weill, 1997; Sharma, 2012; Urbach et al., 2013). For instance, an effective use of IT improves work processes, enhances coordination and collaboration between the various stakeholders, and enables new business models. Hence, IT provides organizations a significant competitive advantage (Broadbent and Weill, 1997; ITL Education Solutions Limited, 2005; Lazic et al., 2011; Sharma, 2012; Urbach et al., 2013).

However, organizations should know how to manage as well as govern IT. For instance, as stated by various authors, organizations that governed badly their IT noticed a decrease in their business growth (Weill and Ross, 2004; Sharma, 2012). Hence, before explaining the importance of IT governance, we will start by defining the concept of governance.

# II. Governance

## 1. What is Governance?

The concept of governance has been present in politics as the synonym for government and defined as "*the act or process of governing, specifically authoritative direction and control*[6]". It is especially defined by international agencies (UNDP, UNESCO, DAC, etc.) as managing the economy of a country by exercising authority and power. However, researchers argue that the definition of governance is broader than a government. The term governance has been then defined as having the organization's governing party distribute power, establish policies, implement them, and then continuously monitor them. Organizations, similarly to countries, cannot function in the absence of governance. It, hence, plays a primordial role in the existence and survival of the organization.

## 2. The Need for Governance in Organizations

While implementing governance helps organizations achieve their business objectives, lacking governance could cause their failure. Countries that are not ruled or governed correctly end up in a massive chaos. A myriad of examples, throughout the history, can illustrate that fact. Similarly, an organization that does not possess proper governance would end up bankrupted and ruined[7]. Before going further in discussing the various aspects of governance in organizations, it seems important to define our concept of an organization. We drew on Alter (2002) where organizations are considered as a coordination of work systems established to reach the goals that these systems cannot reach on their own.

## 3. Levels of Governance

### 3.1 Corporate Governance

Organizations are constituted of complex systems that are not easy to govern. Therefore, governing an organization exists in the form of different levels. The first level of governance is corporate governance. According to Charreaux (1997), corporate governance encompasses

[6] Understanding the Concept of Governance, https://www.gdrc.org/u-gov/governance-understand.html

[7] https://www.theatlantic.com/magazine/archive/2003/12/how-to-kill-a-country/302845/

the organizational mechanisms that define the leaders' powers and influence their decision making. Charreaux continues by stating that these mechanisms are responsible for governing the leaders' conducts while defining their discretionary space. Corporate governance is the way an organization is controlled, administered, and directed through the use of defined processes, laws, policies, and customs. It encompasses the relationship between the organization's different stakeholders, such as, the shareholders, the board of directors, management, clients, employees, regulators, suppliers, creditors, etc. (Charreaux, 1997; Sharma, 2012). This is mirrored by the agency theory (Eisenhardt, 1989) representing the relationships between the principal actor and the agent actor in an organization and reflecting risk-bearing costs as well as efficient organized information.

The most important objective of corporate governance would be ensuring the accountability of few stakeholders through eliminating the principal-agent problem (agency theory) (Jensen and Meckling, 1976). As noted by Sharma (2012), good corporate governance principles must have honesty, integrity, responsibility, mutual respect, and commitment as vital key elements. Other principles are based on ethical behaviors, other stakeholders' interests, shareholders' rights, as well as disclosure and transparency. *De facto*, corporate governance covers all the various business aspects (human resources department, marketing department, finance department, etc.) As noted by several authors (Van Grembergen and De Haes, 2009; Wilkin and Chenhall, 2010; Héroux and Fortin, 2012), corporate governance encompasses IT governance.

## 3.2 IT Governance

### 3.2.1 What is IT Governance?

In line with the understanding of corporate governance stated by the previous studies, several definitions for IT governance emerged, summarized in Table 1. Starting with Van Grembergen & De Haes (2009, p. 3) who define IT governance in terms of "*processes, structures and relational mechanisms in the organization that enable both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from IT-enabled business investments*". Sambamurthy and Zmud (1999) affirm that IT governance focuses on the accountabilities regarding the decision processes carried out as well as the policies guiding these processes. Similarly, Simonson and Johnson (2006, p. 1) also define IT governance as concerning "*IT decision-making, that is, preparation for* *making and implementing decision regarding goals, processes, people and technology on a tactical and strategic level*". However, after additional research, Sambamurthy and Zmud (2000) restate that IT governance does not only focus on the decision making processes, however, it also focuses on the mechanisms in order to make strategic IT decisions. In addition, Peterson (2004, p. 7) also agrees that "*IT governance describes the distribution of IT decision-making rights and responsibilities among different enterprise stakeholders, defining the procedures and mechanisms for making and monitoring strategic IT decisions*". On the other hand, Van Grembergen (2002, p.1) state that IT governance "*refers to the organizational capacity exercised by the board, executive management and IT management in formulating and implementing IT strategy, as this brings together business and IT*". The ITGI (2003, p. 11) agrees with Van Grembergen (2002), where they affirm that IT governance is actually "*the responsibility of the board of directors and executive management*". Furthermore, Webb et al. (2006, p. 7) stated that IT governance referred to "*the strategic alignment of IT with business, aiming to release maximum business value through the development and maintenance of effective IT accountability, performance and risk management*". Many more definitions are found in the literature sharing similar concepts to the ones mentioned above.

All of these definitions can be classified into various groups. First, researchers see that IT governance focuses on allocating the different loci of decision-making rights and accountabilities within an organization (Sambamurthy and Zmud, 1999; Weill and Woodham, 2002; Simonson and Johnson, 2006). They state that IT governance mostly focuses on the distribution of decision rights and responsibilities for an effective use of IT resources. Others see that IT governance is more involved in the strategic alignment between business and IT. According to Webb et al. (2006), IT governance is responsible for maximizing business value through implementing an effective strategic alignment. They also emphasize the effective control of resources, risk, and performance management. On the other hand, IT governance may be thought of as the IT organization of structures and processes seeking to achieve the strategy of the organization (Korac-Kakabadse and Kakabadse, 2001; Van Grembergen and De Haes, 2009). Moreover, Van Grembergen (2002), Parent and Reich (2009), Jewer and McKay (2012), and the ITGI (2003) agree that IT governance is actually the responsibility of the board of directors and executives. Finally, some others then argue that IT governance does not only focus on allocating the decision rights and accountabilities, but it also focuses on addressing these decisions and implementing them through the use of different governance mechanisms (Luftman and Brier, 1999; Sambamurthy and Zmud, 2000; Peterson, 2004; Weill, 2004).

In addition, Musson (2008) state that IT governance is better cited as corporate governance of IT since it indicates that IT governance is actually a joint process of business and IT. Regarding the roots of IT governance, it is thought that it is the descendent of corporate governance and IT management. IT management actually emphasizes managing IT services and IT operations, where IT governance goes much further than this definition (Van Grembergen et al., 2004; Peterson, 2004). Moreover, According to Musson (2008), three IT governance concepts exist in the literature; IT governance as a framework, IT governance as IT decision-making, and IT governance as a branch of corporate governance. We mostly focus in our research work on the second concept identified by Musson (2008): IT governance as IT decision-making.

For the focus of this research work, we adopt the common IT governance definition cited by Luftman and Brier (1999), Sambamurthy and Zmud (2000), Peterson (2004), and Weill (2004) where IT governance focuses on allocating the different decision makers through the use of governance mechanisms (decision-making structures, business processes, and relational mechanisms). This definition covers several aspects of IT governance that are useful for our research work.

**Table 1: IT Governance definitions**

| **IT Governance Definitions** | **References** |
|---|---|
| Allocation of the different loci of decision-making rights and accountabilities. | Sambamurthy and Zmud (1999); Weill and Woodham (2002); Simonson and Johnson (2006) |
| Maximization of business value through implementing an effective strategic alignment | Webb et al. (2006) |
| Mechanisms seeking to achieve the organization’s strategy | Korac-Kakabadse and Kakabadse (2001); Van Grembergen and De Haes (2009) |

| | |
|---|---|
| Responsibility of the board of director and executives | Van Grembergen (2002); ITGI (2003); Parent and Reich (2009); Jewer and McKay (2012) |
| Allocation of decision rights and use of mechanisms to deploy these decisions | Luftman and Brier (1999); Sambamurthy and Zmud (2000); Peterson (2004); Weill (2004) |

### 3.2.2 Why is IT Governance Important?

Studies show that organizations lacking effective IT governance tend to collapse, lose their competitive advantage as well as fail the development of their projects (Ali and Green, 2012). While the link between IT governance and competitive advantage is growing, boards of management and executives of an organization approve of the need to implement effective IT governance (Weill and Ross, 2004). The importance of IT governance has been present in the literature since the 1960s due to Garrity (1963) who first found a positive impact of IT governance on the organization's performance. After Garrity's results, researchers as well as practitioners began to emphasize the need to connect the business strategy with IS strategy while linking business to IS (Galliers and Leidner, 2003). Moreover, several authors show that implementing effective IT governance enhances the organization's performance (Weill and Ross, 2004), its competitiveness (Rau, 2004), its business and IT alignment (Van Grembergen and De Haes, 2009), its costs and risks reduction (Parent and Reich, 2009), in addition to its increased security (ITGI, 2003). For instance, the ITGI (2003) affirms that more than 80% of Chief Information Officers (CIOs) acknowledge the need for a more effective IT governance. Weill and Ross (2004) support this by stating that organizations implementing an effective IT governance have profits that are 40% higher than others. In addition, "improving IT governance" was listed as the third most important priorities by Gartner's *Top Ten CIO Management Priorities for 2003*.

### 3.2.3 Domains Covered by IT Governance

As mentioned earlier, IT governance aims at ensuring effective and efficient use of IT while meeting the organization's objectives. IT governance spreads across five key areas of an organization (Urbach et al., 2013; Buckby et al., 2008; Musson, 2008; Webb et al., 2006; De Haes and Van Grembergen, 2006; Meyer et al., 2003; ITGI, 2003); strategic alignment and value delivery (strategic governance), risk management and resource management (management governance), and performance measurements (operational governance). The strategic governance consists of implementing an effective strategic alignment between IT and business objectives, while delivering value. The second area of IT governance is management governance; it is responsible for managing the risks and resources in the organization. Lastly, the third area of IT governance is measuring the performance of the organization. For instance, Sharma (2012) states that while IT governance drivers are strategic alignment, resource management and performance management, its outcomes are value delivery and risk management. Figure 4 represents the different areas constituting IT governance.

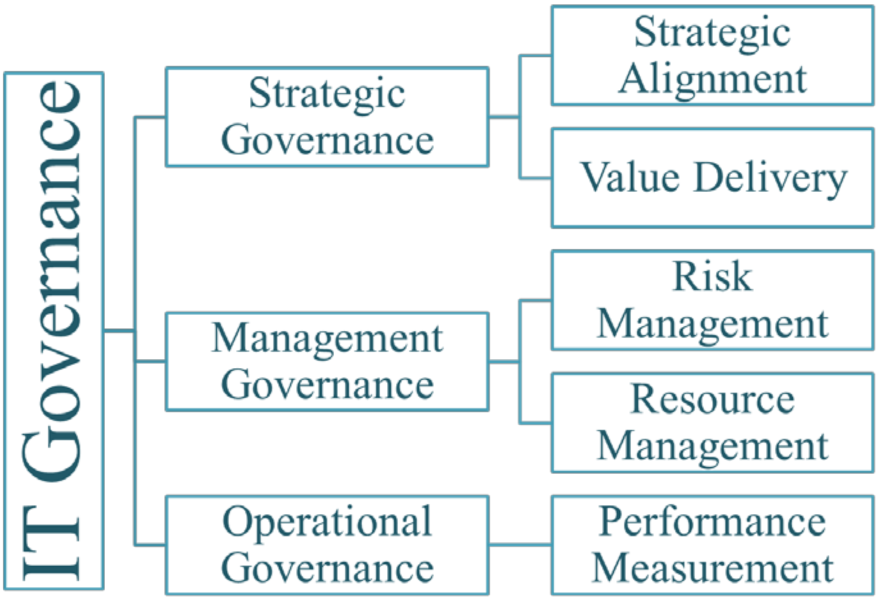


**Figure 4: IT governance domains**

i. Strategic Governance

a. Strategic Alignment

Strategic alignment is defined as "*whether an enterprise's investment in IT is in harmony with its strategic objectives and thus building the capabilities necessary to deliver business value*" (ITGI, 2003, p. 22). Strategic alignment ensures that IT assets are used efficiently to assist the whole organization. It supports organizations in better structuring their business and IT processes. It also leads to business profitability while achieving synergy in the organization. In addition, it maximizes the return on IT investments, it helps achieve competitive advantage through IS and it provides flexibility as well as direction to new opportunities (Avison et al., 2004). It can be accomplished through processes such as strategic IS planning and implementation of frameworks. To obtain a successful strategic alignment between business and IT, the literature states that business executives must "*mesh things from the start*" as well as "*intertwine technology and business processes*" (Keen, 1993, p. 21). According to a study fulfilled by Tallon and Kraemer (2003), alignment is the highest in operations, production and customer relations. However, it is the lowest in marketing and sales, where business and IT managers do not share the same objectives. Nevertheless, the strategic alignment between IT and business needs is still an area of concern. Surveys throughout the past decade showed that IT and business alignment is still the number one concern for businesses[8]. There are opposite opinions concerning this alignment. Some researchers think that it is related to IT requirements matching with business needs (Gordijn & van Eck., 2005), while others affirm it is actually a mutual influence between business and IT (Poels, 2006). As stated by Weill and Broadbent (1998), one should not mix alignment with being just a state or an event; alignment is actually a long journey for organizations. Plus, the literature evokes that business and IT alignment implicates many factors (Enns et al., 1997; Reich and Benbasat, 1996; Broadbent and Weill, 1991) such as, communication and understanding between business and IT executives, the linked business and IS missions, the interconnected business and IS planning processes and results, and the business executives commitment to the IS issues and initiatives. However, to have an effective strategic alignment in the organization, several strategic alignment frameworks have been developed since the appearance of the first Strategic Alignment Model (SAM) implemented by Henderson and Venkatraman in 1991. SAM is based on the strategic fit between external (business strategy and IT strategy) and internal (business infrastructure and IT infrastructure) views as well as the functional integration between technology and organizational views. SAM was then extended by applying it to specific organizations or by reviewing the elements of each domain (Henderson & Venkatraman, 1993; Henderson et al., 1992). In addition, Luftman et al. (1993) formed the Strategic Alignment Framework by further developing the SAM. Moreover, Papp (1999) identifies several financial measures to improve the strategic alignment in organizations while others (Burn and Szeto, 1999; Avison et al., 2004) support the SAM and its structures. New

[8] http://www.information-management.com/photo_gallery/1_26/it-business-alignment-key-barc-survey-10021315-1.html

alternative models arise with Smaczny (2001) where he states that fusion between business units and IT leaders as well as synchronization between business units and the enterprise would lead to a more efficient and effective alignment. It is the level of fusion that distinguishes one organization from another. Kearns and Lederer (2003) implemented a model where they found out that information-intensive organizations have stronger strategic alignment. In addition, Strnadl (2006) fills the gap between business and IT with a model designed with four layers of processes, services, information and technology integration. According to Luftman and Brier (1999), business and IT alignment seems to be a state resulting of the relationship between the business and IT executives. This relationship is measured as a maturity level of six fundamental strategic alignment criteria (communications, competence, governance, partnership, technology scope, and skills), based on Luftman's (2003) Business and IT Alignment Model. The level of maturity shows the capability of an organization to align their IT with their business needs. This model is then tested by Silvius (2007) on several international organizations. It is shown that the higher the level of maturity of these criteria is, the better the business and IT are aligned. Avison et al. (2004) develop a framework determining current alignment levels in the organization. Many other authors address the strategic alignment topic (Bruce, 1998; Maes et al., 2000, Croteau & Bergeron, 2001; Gold, 2002, Peak & Guynes, 2003; Bergeron et al., 2004; Cumps et al., 2006; Wagner et al., 2006; Van Grembergen et al., 2007; Beimborn et al., 2007, etc.).

b. Value Delivery

According to the ITGI (2003, p. 24), value delivery is "*the on-time and within budget delivery of appropriate quality, which achieves the benefits that we were promised*". It is the link between organizational performance and delivery of value from IT systems, in addition to the distinction between the potential value and the realizable value of these systems (Buckby et al., 2008). Value delivery can be achieved via standards such as ITIL, and by relational mechanisms such as staff training. However, research related to IT value delivery is not as present as the one on strategic alignment. Davern and Kauffman (2000) present the elements of the IT value creation process via a theoretical model they create. This model studies the relationship between IT value delivery, IT impacts, and IT management. It represents a first contribution to the IT value delivery literature. Sircar et al. (2000) develop a framework that examines the links between IT investments in an organization and its performance. Moreover, Menon and Lee (2000) state that IT value delivery is actually links between allocative, overall and technical efficiencies while Tallon et al. (2000) discover, through a process oriented model, that strategic alignment and IT investment evaluation play an important role in the organization's performance and value. The literature witnesses an extremely important and interesting research paper regarding IT governance: Weill and Ross (2004). After examining 256 organizations in 23 different countries, they identify several characteristics of top performers such as clear business objectives, engagement, leadership involvement, differentiated business strategies, etc. (Weill and Ross, 2004). Furthermore, a contradiction is found in the literature between Gregor et al. (2006) and the ITGI (2005). The ITGI (2005) proposes that IT value delivery is an in-house method, while Gregor et al. (2006) contradict this statement by affirming that IT delivery value is independent of industry type or size. A set of more elaborated research exists in the literature regarding the IT value delivery topic (Thatcher and Pingry, 2007; Tallon, 2007; Kwon and Watts, 2006; etc.)

ii. Management Governance

a. Risk Management

In addition, ITGI (2003, p. 27) defines risk management of IT systems as "*the extent to which IT assets are protected and the level of assurance required*". Literature about risk management gathered momentum in the last decade. The focus in this area concerns the development of conceptual models on the factors associated with IT risks. In the academic literature, one can find research about risk identification, risk management, and risk assessment. Regarding the research about risk identification, it mostly focuses on outsourcing, IT projects and security risks. Bahli and Rivard (2005) develop risk factors (transaction risks, supplier and client risks, etc.) associated with outsourcing IT operations. Benvenuto and Brand (2005) develop a generic risk assessment model after identifying the different drivers of outsourcing while Gewald and Helbig (2006) develop a model to mitigate outsourcing risks. In addition, many researchers focus on security risks (Broadbent, 2003; Von Solms and Von Solms, 2004; Chapin and Akridge, 2005; Pironti, 2006; Ross et al., 2006). Regarding IT risk management research, it focuses on the identification of main risk factors and the development of risk measures. Young and Jordan (2002) propose that risk management must be considered from the lowest decision making level to the board level. Levine (2004) states that board members are getting aware of the importance of risk mitigation. This is increasing the spending for risk management. Concerning the research on IT risk assessment, Sun et al. (2006) develop a risk assessment model that focuses on incorporating IT risks while promoting methods to manage them. Hinz and Malinowski (2006) also develop a risk assessment model that focuses on problem solving in personal networks. IT risk management research is still developing (Pareek, 2006; Gerber & Von Solms, 2005; Stewart, 2004; COSO, 2004; Standards Australia, 2004; etc.); thus more key issues must be tackled in future research.

b. Resource Management

The ITGI (2003, p. 28) defines resource management as "*the optimal investment use and allocation of IT resources in servicing the needs of the enterprise*". Research concerning resource management has been available for the past 25 years and it addresses different focus areas including IT architecture models, IT governance models, IT steering committees, IT project management, etc. Several researchers studies the impact of IT structure models (centralized, decentralized, federal) and the IT decision making processes of organizations (Sambamurthy & Zmud, 1999; Peterson et al., 2000; etc.). However, Peterson (2004) states that, regardless of the IT structure models, the most important issue for good governance is good IT resource coordination. On the same note, Schwarz and Hirschheim (2003) argue that in order to achieve good IT governance, IT resources must be managed optimally. Ribbers et al. (2002) tackle a new approach of IT resource management by studying the social and procedural mechanisms of IT governance. Moreover, Powell and Yager (2004) take two IT groups in the same organization to study their differences (including their IT structures and coordination mechanisms). However, they could not fully explain the differences, and thus, they state that culture, structure, internal economy, metrics, rewards, methods and tools are important IT governance resources (Powell & Yager, 2004).

iii. Operational Governance

a. Performance Measurement

The ITGI (2003) defines performance measurement as "*tracking project delivery and monitoring IT services*" (p. 29). Research about performance measurements include development of measurement methods and tools such as the IT balanced scorecard (ITBSC) (i.e. a strategic planning and management system used worldwide in organizations aiming at aligning business activities with the strategy and vision of the organization, monitoring their performance against strategic goals, and improving external as well as internal communications (Balanced Scorecard Institute[9]) and maturity model assessments). Van Grembergen and Van Bruggen (1997) show the way balanced scorecards can measure the IT department's contribution to the business. Then, Van Grembergen and De Haes (2005) use the ITBSC to develop an IT governance balanced scorecard (ITGBSC). Researchers, then, use this ITGBSC to examine properly the relationship between structures, processes and relational mechanisms. In addition to that, performance measurement focuses also on implementing Key Performance Indicators (KPIs) as well as developing measurement frameworks including the COBIT, ITIL, ITSM, etc.

Table 2 represents a summary of the principles of each IT governance domain.

**Table 2: Principles of IT Governance domains – Based on Fletcher (2006)**

| **IT Governance Domains** | **Principles** |
|---|---|
| Strategic Alignment | - Competitive advantage (Avison et al., 2004)<br>- IT investments align with organization objectives (Avison et al., 2004)<br>- IT strategy aligns with organization strategy (Reich and Benbasat, 1996)<br>- IT operations align with organization operations (Tallon and Kraemer, 2003) |
| Value Delivery | - Quality (ITGI, 2003)<br>- On-time<br>- Within budget<br>- Benefits promised |
| Risk Management | - Existing risks monitored (ITGI, 2003)<br>- Risks mitigated<br>- Risks transferred to insurance coverage |
| Resource Management | - IT resources used optimally (ITGI, 2003)<br>- Internal and external IT services monitored<br>- Human resources and technical resources managed |
| Performance Management | - Clear goals defined (ITGI, 2003)<br>- Good measures defined |

### 3.2.4 IT Governance Types and Contingency Factors

IT governance in an organization can be centralized, decentralized, or federal, depending on the location of its decision-making authorities. While centralized IT governance gives all

[9] http://www.balancedscorecard.org/BSC-Basics/About-the-Balanced-Scorecard

decision-making authorities to the central IS body allowing a greater control over IT processes, decentralized IT governance distributes authority to different business units (Brown, 1997). Meanwhile, a federal IT governance gives authority to the IS body as well as to business units. The choice of IT governance type (centralized, decentralized, or federal) is affected by various contingency factors.

i. Contingency Factors

Several researchers study the impact of contingency factors on IT governance. These factors include, the firm size – large organizations, SMEs, microbusinesses – (Starre and de Jong, 1998; De Haes & Van Grembergen, 2006; Ahituv et al., 1989; Brown and Magill, 1994; Clark, 1992; Tavakolian, 1989; Weill, 2004; Sambamurthy and Zmud, 1999), the geographical location – North America, Central and South America, Europe, Middle East and Africa, Asia and Oceania, or Global – (Starre and de Jong, 1998; Brown and Magill, 1994; De Haes and Van Grembergen, 2006; Sambamurthy and Zmud, 1999), the sector – public or private sector (De Haes and Van Grembergen, 2006), the industry sector – Finance, IT services, Health, Manufacturing, Other – (De Haes and Van Grembergen, 2006; Ahituv et al., 1989; Clark, 1992; Weill, 2004), corporate governance structure – centralized, decentralized, or federal – (Starre and de Jong, 1998; Ahituv et al., 1982; Applegate et al., 1996; Brown and Magill, 1994; Tavakolian, 1989; Weill, 2004; Sambamurthy and Zmud, 1999), the governance experience – between low and high experience in governance – (Weill, 2004), economies of scope – level of sharing appropriate IT related expertise and investments across the organization – (Sambamurthy and Zmud, 1999; Boynton et al., 1992; Brown and Magill, 1994) and the corporate strategy – cost focused, innovation focused (Brown and Magill, 1994; Tavakolian, 1989; Weill, 2004). In addition, Brown and Grant (2005) identify organizational maturity as a factor affecting IT governance. Figure 5 represents the different contingency factors found in the literature, affecting the choice of IT governance type.

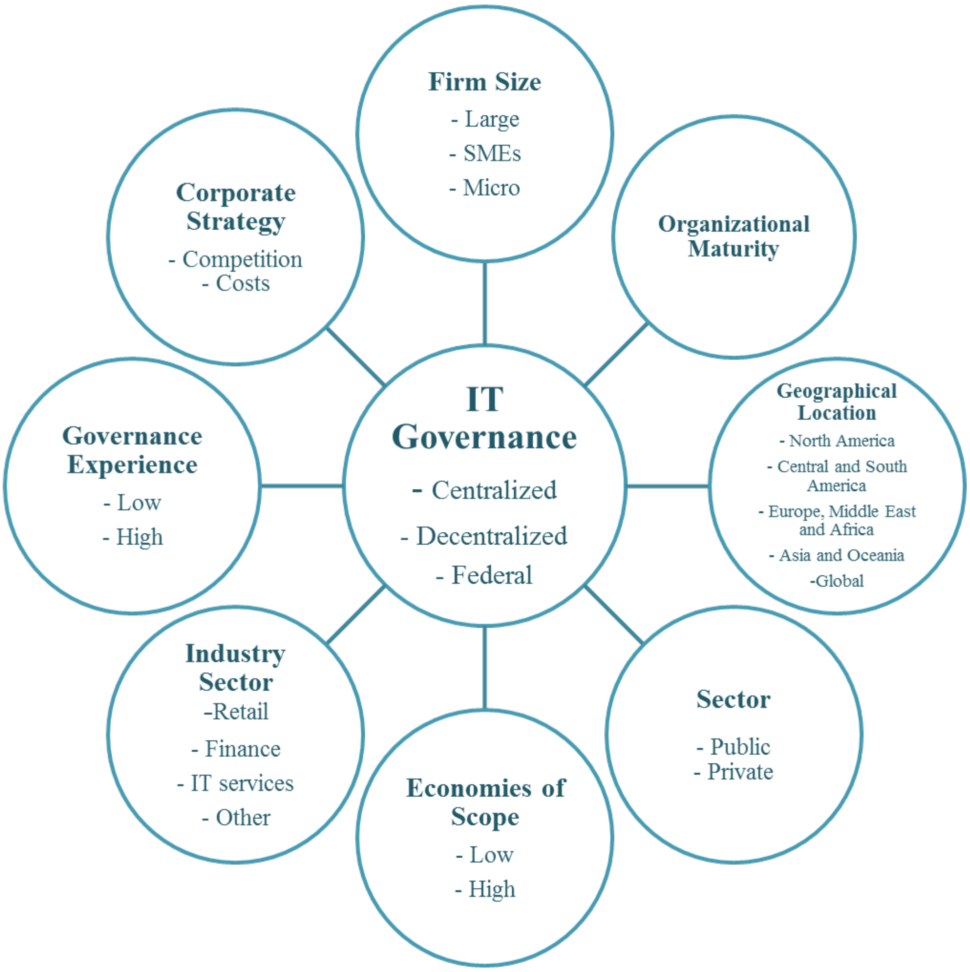


**Figure 5: Contingency factors**

ii. Effect of Contingency Factors

Based on the previously cited authors, centralized IT governance is mostly related to the following contingency factors: being an SME following a cost focused business strategy (economies of scale), having centralized business governance, a low information intensity (i.e. amount of information processing that is required to acquire, process and then deliver the product in its final form to the users), a stable environment and a low business competency where their main decision rights and IT decisions are made by senior IT leaders (Brown and Magill, 1994; Peterson, 2004; Weill, 2004; Gu et al., 2008; Peterson, 1998). In fact, until the 1960s, the most dominant location of decision-making authorities was centralized. This governance emerged from having central computers in the 1960s, which pushed organizations to perform their data analysis centrally (Olson and Chervany, 1980). Therefore, traditional organizations tend to place their decision-making authorities in a centralized IS body (Boynton and Zmud, 1987).

On the other hand, decentralized IT governance is mostly used by large organizations, following an innovation focused business strategy, decentralized business governance, high information intensity, an unstable environment, and a high business competency where their IT decision rights and IT capabilities are made by the business units (segment of an organization representing a specific business function) (Brown and Magill, 1994; Peterson, 2004; Weill, 2004; Gu et al., 2008; Peterson, 1998). While comparing the difference between centralization and decentralization, Lorsch and Lawrence (1970) state, "… *it is not just a question of dividing responsibility up and down the hierarchy, but it is also a question of organizing the flow of information and coordinating devices*". In addition, the literature showed that organizations aiming at having multiple competing objectives adopt federal IT governance (Brown and Magill, 1994; Peterson, 2001; Sambamurthy & Zmud, 1999), since organizations should focus on standardization as well as innovation. However, the federal IT governance is a complex system that involves several stakeholders with different perspectives and motivations. Even if each stakeholder is correctly pursuing their own strategic objectives, they might be blind regarding some sides, which will highly affect IT governance. In addition, the federal type involves different forms of allocating the different IT decision making authorities. Hence, with the federal model, coordination between the different parties in the organization is essential. Table 3 recapitulates some contingency factors and their proven effects on the IT governance type. The contingency factors leading to a federal IT governance type fall in between the centralized and decentralized ones.

**Table 3: Effects of contingency factors – Based on Peterson (1998)**

| **IT Governance Type** | **Firm Size** | **Corporate Governance** | **Corporate Strategy** | **Information Intensity** | **Stability** | **Skills and Competences** |
|---|---|---|---|---|---|---|
| **Centralized** | Small | Centralized | Cost Focus | Low | High | Low |
| **Decentralized** | Large | Decentralized | Innovation Focus | High | Low | High |

iii. Interaction and Effect of Multiple Contingency Factors

Many authors analyze the way the previously mentioned contingency factors shape the organization's IT governance procedures while interacting with each other (Samburthy and Zmud, 1999; Brown and Grant, 2005; Gu et al., 2008, Adams et al., 2008). Samburthy and Zmud (1999) were the first authors to address the effects multiple contingencies interactions have on IT governance types. Their theory states that the contingency factors interact with each other by diminishing, intensifying, or overruling their mutual influences on the IT governance type. Sambamurthly and Zmud's (1999) article also aims at proving 3 hypotheses. They claim and then prove that if an organization's multiple contingencies are amplifying their mutual influence on IT governance – hence reinforcing one another – then, its IT governance is either centralized or decentralized. Similarly, if the multiple contingencies interacting are overriding their mutual influence on IT governance – hence one is dominating the other – then, its IT governance is also either centralized or decentralized. However, if their multiple contingencies are dampening their mutual influence on IT governance – hence they are conflicting with one another – then the organization should adapt a federal IT governance type.

To illustrate these hypotheses, we can take the example of an organization possessing the following contingency factors: a decentralized corporate governance and a low level of sharing IT expertise (low economies of scope, leading to a centralized governance). If the corporate governance factor is dominating the economies of scope one, the organization would have a decentralized IT governance; following the governance type of the dominating factor. On the other hand, imagining an organization having these contingency factors: being an SME (most probably leading to a centralized governance), a centralized corporate governance, and a high level of sharing IT expertise (high level of economies of scope, leaving to a decentralized governance). While the effect of these three contingency factors are dampening, thus conflicting with each other, the organization will adopt a federal IT governance type, according to the proven hypotheses of Sambamurthy and Zmud (1999). Figure 6 represents the mediating effect contingency factors have on the IT governance outcomes.

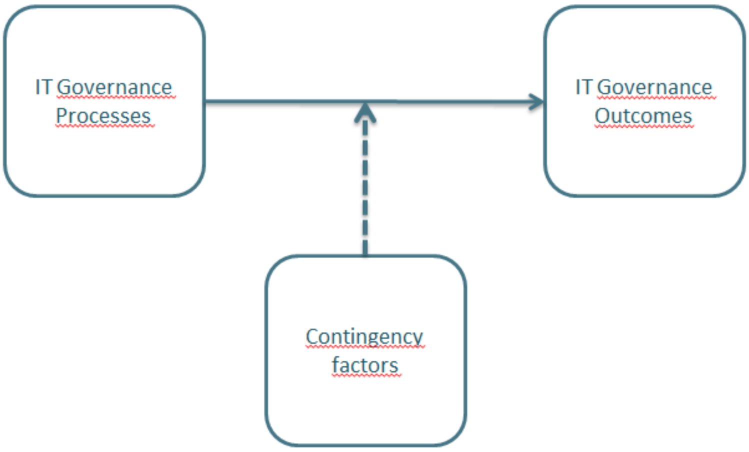


**Figure 6: Effect of multiple contingency factors – Based on Ribbers et al. (2002)**

### 3.2.5 Implementing IT Governance

Building an IT governance model is an important and popular subject in the IS literature due to the various benefits brought by such models. Several researchers propose a specific model for governing IT.

Weill and Ross (2004) propose an IT governance model after interviewing 256 organizations located in several continents. They affirm that building an IT governance model starts with addressing the various IT decisions, followed by allocating the appropriate decision makers, and finally governing these decisions through a set of mechanisms (decision-making structures, business processes, and relational mechanisms). Van Grembergen and De Haes (2004) also propose governing an organization's IT through the implementation of various mechanisms. In addition, Korac-Kakabadse and Kakabadse (2011) state that IT in an organization is best governed through a stakeholder model, focusing on the different stakeholders impacted by IT. They agree with Weill and Ross (2004) stating that in order to achieve the business objectives, IT governance should also focus on the various structures, processes, and relational mechanisms.

Therefore, in addition to the various contingency factors affecting the type of IT governance implemented, building an IT governance model relies on implementing appropriate governance mechanisms by the most suitable decision makers.

### 3.2.6 IT Governance Components

i. IT Governance Decisions

IT principles, IT architecture, IT infrastructure strategies, business application needs, and IT investment and prioritization constitute the five major IT decisions that organizations, specifically large ones, address (Weill, 2004). IT principles represent simple statements stating an organization's beliefs concerning the way to use IT on the long term. Such principles are deployed as a communication bridge between technical IT professionals and top managers (Davenport et al., 1988). Additionally, IT architecture refers to a set of detailed standards and policies responsible for the design of infrastructure technologies, applications and databases leading to the way to implement business (Ross, 2003). It also discusses the way core business processes are implemented in IT (Musson, 2008). IT infrastructure strategies constitute a set of reliable and centrally coordinated strategies organized by human and technical IT capabilities and budgeted by senior managers, including help desk, shared data and networks (Ross and Weill, 2002). Another major IT decision is related to the business application needs where these needs are satisfied by internally developed IT services or outsourced ones. The fifth major IT decision is regarding the IT investment and prioritization. Such decisions are concerned with the amount and the place to invest in IT. It is important to implement on the different IT governance levels; whether it is how much to invest for a more advantageous business-IT alignment, for more effective risk mitigation or for a better performance (for e.g. through implementing frameworks such as COBIT, ITIL, ISO/IEC 27001, etc.)

ii. IT Governance Decision Making

a. Types of Decision Rights

Appropriately allocating IT decision rights between business and IT departments remains a serious challenge in the 21$^{st}$ century (Brown and Grant, 2005). When it was easy for traditional organizations to allocate all decision rights to their IT center, this becomes a hard and complicated task today. According to many authors, decision rights of an IS project are divided into two parts; decision control rights (DCR) and decision management rights (DMR) (Fama and Jensen, 1983; Jensen and Meckling, 1995; Tiwana, 2009). For instance, Fama and Jensen (1983) identify four activities addressed through the decision control and management rights; ratification, monitoring, initiation, and implementation. DCR encompass ratification – the approval of the initiatives implemented in the future – and monitoring – the different implementation and specification of performance measurement criteria. However, DMR incorporate the initiation – using the organization's resources in making decisions – and the implementation – the execution of the ratified decisions (Fama and Jensen, 1983). Table 4 represents the different types of decision making present in the literature.

**Table 4: Types of decision rights**

<table>
<tr><th>Type of decision rights</th><th>Examples</th><th>References</th></tr>
<tr><td>DCR (ratification, monitoring)</td><td>Establishing rewards and penalties for project outcomes<br>Implementing mechanisms to evaluate project team’s performance<br>Specifying project milestones and deliverables<br>Monitoring project progress</td><td rowspan="2">Fama and Jensen (1983)<br>Jensen and Meckling (1995)<br>Tiwana (2009)</td></tr>
<tr><td>DMR (initiation, implementation)</td><td>System design<br>Software architecture design<br>Selection of a software platform<br>Development methodology<br>Programming languages<br>Definition of application features</td></tr>
</table>

b. Decision Making Criteria

According to Reix et al. (2016), making a decision is influenced by three types of rationalities: calculating the profitability of the decision, stating the positive characteristics of the decision, or imitating other successful organizations. However, if an organization wants to base its decision only on calculating its profitability, it will have to disregard several factors, including the psychology of the decision-maker (whether he’s receptive, perceptive, analytical, intuitive, etc.), organizational constraints, the weight of the compromise (price of building coalitions), and the context of the decision making (the organization is in a crisis, it has an opportunity, it needs to drift apart, etc.) Even if the organization has to disregard these factors, it can base its decisions on several possible criteria, such as the Laplace criterion (choosing the most profitable scenario), the MiniMax criterion (minimizing the maximal losses, hence choosing the least worst scenario), the Savage criterion (building a regret matrix and then applying the MiniMax criterion), the mathematical expectation criterion (allocating a success probability to each scenario and choosing the scenario with the best results/probability ratio), or even the Bernoulli criterion (choosing the scenario with the highest geometric mean of outcome) (Reix et al., 2016). We will not dig deeper into these approaches as they go beyond the scope of our research. It is although important to note that behind the simplistic façade of making a decision, several criteria and constraints need to be considered.

### c. Decision Makers Allocation

Several researchers have studied the repartition of the decision rights responsibilities between the IT department and the business departments (Ross et al., 1996; Weill and Ross, 2004; Marwaha and Willmott, 2006). Some authors affirm that the board of directors and executives are responsible for the overall scope of IT governance (Jewer and McKay, 2012; De Haes and Van Grembergen, 2008). However, dividing IT decision rights among the different parties of an organization is a hard accomplishment. Traditionally, IT units were viewed as the center of IT decision making, even if several decisions require the presence and collaboration of the different business departments (Ruohonen, 1991; Brown and Magill, 1994; Brown, 1999; Sambamurthy and Zmud, 1999).

However, in order to govern IT, the right decisions must be allocated to appropriate decision-makers among various stages. Xue et al. (2008) state that IT governance should include pre-decision stages. In these stages, the participants are more important than the final decision makers. In addition, the IT department might not play a primordial role in the decision stages, even when the top management's approval is mandatory. Finally, they affirm that the allocation of final decision rights is only a part of IT governance; it is affected by the IT investment level, external environment (competitive pressure, external resources, etc.), and internal context (organizational centralization, IT function power, etc.) (Xue et al., 2008).

Nonetheless, effective IT governance (i.e. one that ensures a better delivery value, risk mitigation, performance, etc.) allocates the right group of people to the right key IT decisions. Tiwana (2009) affirms that if a class of decision rights is decentralized then the business departments are more responsible, however if a class is centralized, then it is the IT department's responsibilities. Moreover, after analyzing 57 IT investment decisions, Xue et al. (2008) outlined seven IT governance archetypes; top management monarchy (business executives), top management IT duopoly (business and IT executives), IT monarchy (IT executives), administration monarchy (administrative departments), administration IT duopoly (administrative departments and IT executives), professional monarchy (business professionals), and professional IT duopoly (business and IT professionals). They add that the decision-making process is moderated across two stages: initiation and development. Nevertheless, Xue et al. (2008) study the IT decision-making process in the healthcare industry only. The fixed contingency factor (industry type) can make the results biased.

Weill and Ross (2004) conversely analyze a higher amount of organizations (256) in different industries and thus, offer more accurate results, regarding decision makers, than Xue et al. (2008). They state that these decision rights are held, in general, by one of six different parties: business monarchy, IT monarchy, feudal, federal, IT duopoly or anarchy. Based on their results, we will define the different decision-making parties. Business monarchy regroups a set of senior business executives, excluding IT executives who take their own decisions and act independently of business executives. However, IT monarchy is a group of IT executives responsible for taking different decisions. Regarding the feudal archetype stated by Weill and Ross (2004), it consists of having each unit making their own decisions in order to optimize their local needs. However, this archetype is scarcely found in organizations since synergies across business units are primordial for them. The federal decision-making archetype attempts to balance multiple governing bodies working on different business hierarchy levels. Furthermore, when decisions are an agreement between IT executives and a business group, it is represented by an IT duopoly archetype. This archetype is divided between an IT and a business representation. The last archetype is anarchy. It is similar to the feudal archetype where each group makes their own decisions based on their needs. The difference is that anarchists speak for small groups where feudal archetypes are for larger groups. The difference between the resulted archetypes of Weill and Ross (2004) and Xue et al. (2008) is also related to the decision making stage. Taking IT duopoly for an example, Weill and Ross (2004) meant that IT professionals make the IT decisions, whereas Xue et al. (2008) meant that IT professionals only initiate and develop the proposals (Decision Management Rights – Fama and Jensen, 1983) while the top management is responsible for the decisions (Decision Control Rights – Fama and Jensen, 1983). Nevertheless, Fama and Jensen (1983), Jensen and Meckling (1995), Kirsch and Beath (1996), Ross et al. (1996), Sambamurthy and Zmud (1999), Weill and Ross (2004), and Tiwana (2009) all agree that decisions rights should not just be allocated to one party. While decision rights should be shared by the IT department and business departments with a greater ownership by one of the two, it remains a complicated task. This is shown in the example of Weill and Ross (2002) where they identify executive decisions related to the quality of IT services, what qualifies security risks and who is responsible for IT failure. However, since these decisions affect business' strategy, they should be made by senior managers instead of the IT department. This proves that organizations' decision makers differ from one organization to the other.

#### iii. IT Governance Mechanisms

Based on the IT governance definition chosen in this research work, IT governance does not only focus on allocating the appropriate decision-makers authorities, but also on the execution of these authorities through the use of decision-making structures, business processes, and relational mechanisms. Identifying a good combination of mechanisms is a hard and complex task differing from one organization to the other (Cognizant, 2013; Lee and Lee, 2008; Musson, 2008; Bhattacharjya and Chang, 2006; Johnstone et al., 2006; Weill, 2004). Table 5 represents a summary of the most cited mechanisms in the previous studies. It is mostly based on the key IT governance mechanisms used by top-performing organizations (Weill and Ross, 2004), mechanisms positively influencing the implementation of effective IT governance (Ali and Green, 2012), and the most important IT governance mechanisms cited by De Haes and Van Grembergen (2009).

##### a. Decision-Making Structures

Decision-making structures are the organizational roles and responsibilities for making IT decisions (Peterson, 2004). The most vital IT governance structure is the roles and responsibilities being communicated by the board and clearly understood throughout the organization. In addition, the presence of the CIO on board is very important, where he and the CEO should report to the board on a regular basis. The CIO is part of the senior-level decision making process. Moreover, the presence of IT steering committees as well as IT strategy committees is primordial to manage IT costs, IT priorities, IT resource allocations and to assist the board in overseeing and governing the organization's IT related matters, respectively. In addition, it is important to have a high level of IT expertise at the board of directors' level. Moreover, the presence of IT governance control practices is primordial for achieving the decided IT governance objectives. These control practices might include governance committees and bodies (to help mandate compliance with the IT governance objectives, for example, an architecture review board, investment prioritization committee, project review board, data quality management center of excellence, service management office, independent cloud risk council, etc.) Several others structures help in the implementation of an effective IT governance including, IT councils, IT leadership councils, IT project steering committees, IT audit committee at board of director's level, IT governance officer, business-IT relationship managers, etc. Bhattacharjya and Chang (2006) state that the development of IT governance structures leads to improved processes as well as relational mechanisms.

b. Business Processes

Business processes are defined as arrangements of formal decision making ensuring consistent daily behaviors to the defined IT policies along with the use of various monitoring frameworks and tools (Bowen et al., 2007). IT Balanced Scorecards (ITBSC) are a strategic planning and management system used worldwide in organizations aiming at aligning business activities with the strategy and vision of the organization, monitoring their performance against strategic goals, and improving external as well as internal communications[10]. A primordial process mechanism is the strategic information system planning (e.g. Business System Planning, Critical Success Factors, Competitive forces model of Porter, Business Process Reengineering approach, value chain models of Porter, etc.) aiming at the practical implementation of the strategic alignment within an organization. Using existing frameworks for IT governance is a helpful process mechanism, including COBIT, ITIL, COSO, ERM, etc. Service Level Agreements (SLAs) play an important role, in a maturity IT governance environment, such as defining the levels of services acceptable by users, the mutually agreed upon quality of service indicators, the levels attainable by the service provider, etc. Moreover, organizations can deploy business-IT alignment models such as the strategic alignment model of Venkatraman and Henderson (1991) (SAM), or the models further developed based on SAM. In addition to the strategic alignment models, organizations can measure their governance maturity using IT governance maturity models

[10] http://www.balancedscorecard.org/BSC-Basics/About-the-Balanced-Scorecard

allowing them to grade their maturity level from a nonexistent (0) to an optimized (5) one. This will allow them to benchmark themselves against the best practices and guidelines. More processes can fall under the category of approvals and check controls, which would ensure compliance with IT governance objectives, such as tool-based infrastructure monitoring, periodic and planned baselines for configuration items, application-centric cloud resource accounting, capacity plans fed into the annual budget, etc. (Cognizant, 2013). Other business processes exist, including chargeback, IT budget control and reporting, project governance methodologies, portfolio management (Information Economics, Business Cases, ROI, etc.).

c. Relational Mechanisms

Relational mechanisms, also known as communication mechanisms, complement the structures and processes, and are vital for the sustainability of business-IT alignment (Peterson, 2004). For instance, a high business department technical knowledge positively influences the effective exercise of decision control rights, which also positively influences IS efficiency. In parallel, a high IT department business domain knowledge positively influences the effective exercise of decision management rights, which also positively influences IS effectiveness (Tiwana, 2009). Therefore, a shared knowledge between the business and IT, an active participation by the principle stakeholders, a collaboration between them, partnership rewards and incentives, a business-IT collocation, shared understanding of the different business and IT objectives, a cross functional business and IT job rotation and training, an IT governance awareness campaign, and knowledge management in IT governance constitute important relational mechanisms. In addition, governance meetings and initiatives are important to monitor and track compliance with IT governance, such as periodic business partner review, annual headcount planning, total cost of ownership report, independent project risk review, peer review efficiency reporting, annual infrastructure planning, annual site visits for strategic vendors, big data performance analytics, etc.

**Table 5: Examples of mechanisms**

| Type of Mechanisms | Areas | Mechanisms | References |
|---|---|---|---|
| Structures | IT Executives, committees and councils | IT steering committee | Weill and Ross (2005); Ali and Green (2012); Vaswani (2003); Karimi et al. (2000); ITGI (2003); Nolan (1982); De Haes and Van Grembergen (2009); |

| | | | |
|---|---|---|---|
| | | | Bhattacharjya and Chang (2006); Peterson (2004); Héroux and Fortin (2014) |
| | | IT strategy committee | Weill and Ross (2005); Ali and Green (2012); ITGI (2003); Gottschalk (1999); Premkumar and King (1994); De Haes and Van Grembergen (2009); Bhattacharjya and Chang (2006); Héroux and Fortin (2014) |
| | | Senior management involved in IT | Ali and Green (2012); Rockart (1988); Cerpa and Verner (1998); Earl (1993); Schuman and Rohrbaugh (1991); Sohal and Fitzpatrick (2002); Vaswani (2003); De Haes and Van Grembergen (2009) |
| | | IT leadership decision making body | Weill and Ross (2005); De Haes and Van Grembergen (2009); Bhattacharjya and Chang (2006); Peterson (2004); Héroux and Fortin (2014) |
| | | CIO reporting to CEO and/or COO | De Haes and Van Grembergen (2009); Peterson (2004) |
| | | CIO on executive board | De Haes and Van Grembergen (2009); Bhattacharjya and Chang (2006); Peterson (2004) |
| | | Center of Competency | Peterson (2004); Weill (2004) |
| Processes | Strategic IT monitoring and decision-making | Governance Frameworks (COBIT, ITIL, COSO, etc.) | ITGI (2005); De Haes and Van Grembergen (2006); Lee and Lee (2008) |
| | | SLAs | Weill and Ross (2005); Bhattacharjya and Chang (2006); Peterson (2004) |
| | | Risk management tools | Weill and Ross (2005); |

| | | | |
|---|---|---|---|
| | | | Parent and Reich (2009); Héroux and Fortin (2014) |
| | | IT balanced scorecard | Ali and Green (2012); ITGI (2003); Hardy (2003); Bhattacharjya and Chang (2006); Peterson (2004); De Haes and Van Grembergen (2004) |
| | | Project tracking systems | Ali and Green (2012); Weill and Ross (2005); ITGI (2003); Hardy (2003); De Haes and Van Grembergen (2009); Bhattacharjya and Chang (2006); Peterson (2004); Héroux and Fortin (2014) |
| | | Portfolio management (business cases, information economics, ROI, payback, chargeback) | Ali and Green (2012); Weill and Ross (2005); ITGI (2003); Hardy (2003); De Haes and Van Grembergen (2009); Peterson (2004) |
| | | Strategic information systems planning | De Haes and Van Grembergen (2009); Bhattacharjya and Chang (2006); Peterson (2004); |
| Relational | Shared understanding, partnerships and dialogue | Shared understanding of business and IT objectives | Weill (2004); Bhattacharjya and Chang (2006); Peterson (2004); Héroux and Fortin (2014) |
| | | Cross-functional business and IT job rotations and training | Weill (2004); Bhattacharjya and Chang (2006); Peterson (2004); Héroux and Fortin (2014) |
| | | Joint decision between IT and business | Weill and Ross (2005); Bhattacharjya and Chang (2006); Peterson (2004) |
| | | Awareness | Ali and Green (2012); Beyer and Nino (1999); Trevino et al. (1999); McCabe et al. (1996) |
| | | Partnership rewards and incentives | Peterson (2004); Weill (2004) |

| | | | |
|---|---|---|---|
| | | Communication and closer relationship between business and IT | Ali and Green (2012); Weill and Ross (2005); De Haes and Grembergen (2005); Henderson et al. (1993); Broadbent and Weill (1998); Luftman and Brier (1999); Luftman (2000); Reich and Benbasat (2000); Callahan et al. (2004); Peterson (2004); Héroux and Fortin (2014) |

### 3.2.7 IT Governance in the Digital Age

Running a longitudinal study in large organizations shows the evolution of the role of their IS, from traditional support systems to innovative strategic tools. Continuous and fast innovations, significant improvement of the performance/cost ratio, and increase in demand accelerated this evolution (Reix et al., 2016)

While IT is available for everyone and competitors can easily imitate the innovator's process, competitive advantage is being erased. Thus, several authors wonder whether the competitive advantage achieved through the use of IT is sustainable (Reix et al., 2016; Brown and Grant, 2005; De Haes and Van Grembergen, 2004). Therefore, in today's fast growing environment, Reix et al. (2016) advise organizations to increase their flexibility, their adaptation to changes, and their strategic agility instead of fighting competitors. They add that, rapidly exploiting market imperfection, implementing strategic moves based on innovation, as well as fast repeated organizational transformations are today's strategies basics. These various tactics are all founded on an increased use of IT.

Porter (1982) states that the rules of the competitiveness game are determined by five forces, responsible for building the organization's competitiveness structure. The five forces represent competition between organizations in the same field, power of negotiation with clients, power of negotiation with suppliers, threat of new entrants and threat of substitutes. Porter's five forces are applicable in a stable sector. However, in the new digital sector, where IT constitutes the core of businesses, these five forces are not well applied since boundaries between the different sectors become transparent and open. Thus, Reix et al. (2016) state that today, a sixth force should be added to Porter's (1982) model; entitled the power of the regulatory authority. It represents a reflection of today's industrial reality. To face these forces, organizations would adopt one of the following generic strategies; either a low cost, a differentiation, or a focalization strategy.

For instance, in order to face these six forces, organizations use IT to support and reinforce their strategies. Examples will better illustrate how the use of IT can help organizations. In order to face today's competitiveness; they can reduce their costs through decreasing their conceptual (computer assistance), fabrication (optimization), and distribution (geolocation) costs. If they opt for the differentiation strategy, they can use IT to differentiate products and service by remote maintenance of services, accounts management via the Internet, or by online products customization. Moreover, in order to improve their negotiation and attract more clients, organizations could expand the market through the use of social media, or offer them services to facilitate their orders through online reservations and deliveries, memberships, loyalty cards, etc. In this previous case, customer's loyalty is emphasized. In addition, organizations could improve negotiations with their suppliers by expanding their range of suppliers using IT, and especially the Internet. In order to face the threat of new entrants, organizations could lower their costs (as mentioned earlier), offer better customized products/services, and create entrance barriers. Besides, to face the threat of substitutes, organizations could improve their performance/price ratio in addition to innovate, through applying Computer-Aided Design and Manufacturing (CAD and CAM) to propose various products at reasonable prices. Finally, the newly added force regarding the power of the regulatory authority can highly influence Porter's (1982) forces. It can limit the competitive intensity by fixing norms to each sector.

Therefore, as organizations are adapting to the fast changes in today's digital age, the use of IT is playing an important role. This supports the importance of governing IT effectively, in order to benefit from all of its advantages and the advantages from new technologies, such as cloud computing.

# Second Section: Cloud Computing

## I. History of Cloud Computing

### 1. Evolution towards Cloud Computing

Various concepts led to the emergence of cloud computing throughout these previous years. In the 1960s, the development of the internet pushed the rise of computing utilities provisions. This introduced the new idea of using networks in order to provide computing as a service (Kleinrock, 2005; Cafaro and Aloisio, 2011). Then, in the 1980s the emergence of distributing IT infrastructure through a network began with Application Service Provision (ASP) such as email services provided by Hotmail (Durkee, 2010). This was also known under the name of "Client Server". As the Internet and the network were maturing, the appearance of the "dot-com bubble" started the application outsourcing trend (Susarla et al., 2003). The dot-com bubble event represents the large investment bubble that was created around the Internet, pushing investors to deposit money in organizations possessing a ".com" in their business model (Buenstorf and Fornahl, 2009). Then, few years later, the concepts of grid computing, utility computing, and virtualization on commodity hardware gained popularity as means of coordinating customers' on-demand needs by providing them through large scale computing resources (Foster et al., 2008; Bunker and Thomson 2006; Killalea, 2008). However, we will not define these concepts as they do not fall within the scope of this research work.

After the appearance of such computing concepts, large organization such as Amazon, Google and Microsoft began developing large scale datacenters of commodity hardware. Cloud computing (CC) hence emerged, in terms of technological innovations, such as through datacenter automation (Armbrust et al., 2010), high performance, and virtualization (Quintero et al., 2013) and in terms of service-based perspectives (Vouk, 2008). Nevertheless, cloud computing hence emerged as the transfer of computing activities from private datacenters to large-scale public ones that are accessible over the Internet (Quintero et al., 2013), where the term cloud has begun to describe figuratively the Internet. Furthermore, this emergence pushed the academic and professional literature to address various aspects of CC, from the technological provision details related to cloud services till the revolutionary impact of CC as "a new computing paradigm" (Carr, 2008; Zhang et al., 2010). The evolution towards cloud computing can be summarized in the following Figure 7.

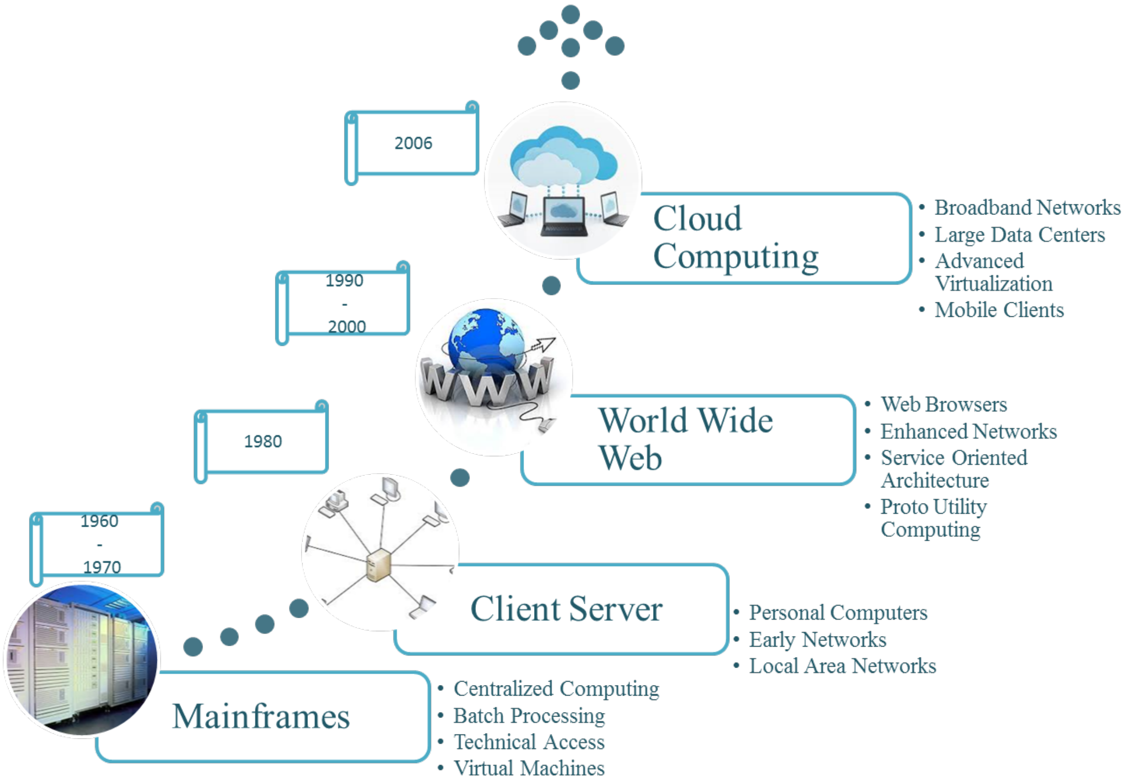


**Figure 7: Evolution towards Cloud Services – Based on the Defense Science Board (2013)**

## 2. Emergence of the Cloud Computing Market

Amazon, a popular online retail organization, was the first to pioneer the CC market, where in 2002 they first launched services to leverage their computing capacities offering online services for external organizations. The Amazon Web Services (AWS) constitute common services for a large list of famous companies[11], including Adobe, Airbnb, General Electric, Netflix, Siemens, Vodafone, etc. Amazon launched in 2006 services that were highly adopted by these companies, such as the Simple Storage Service (S3) and the Elastic Compute Cloud (EC2). The S3 and EC2 solutions offer their clients storage infrastructures as well as software applications. The emergence of cloud solutions continued, few years later, with other well-known organizations such as Microsoft and Google. They offered solutions that are similar to Amazon. Through Google App Engine and Microsoft Azure, these organizations became major cloud solutions providers, offering clients storage capacities in their datacenters. In

[11] https://aws.amazon.com/solutions/case-studies/?nc1=f_ls

addition to these organizations, IBM, HP, Salesforce.com also contributed to the emergence of cloud computing. Based on Su (2011), Figure 8 summarizes the evolution of the cloud computing market.

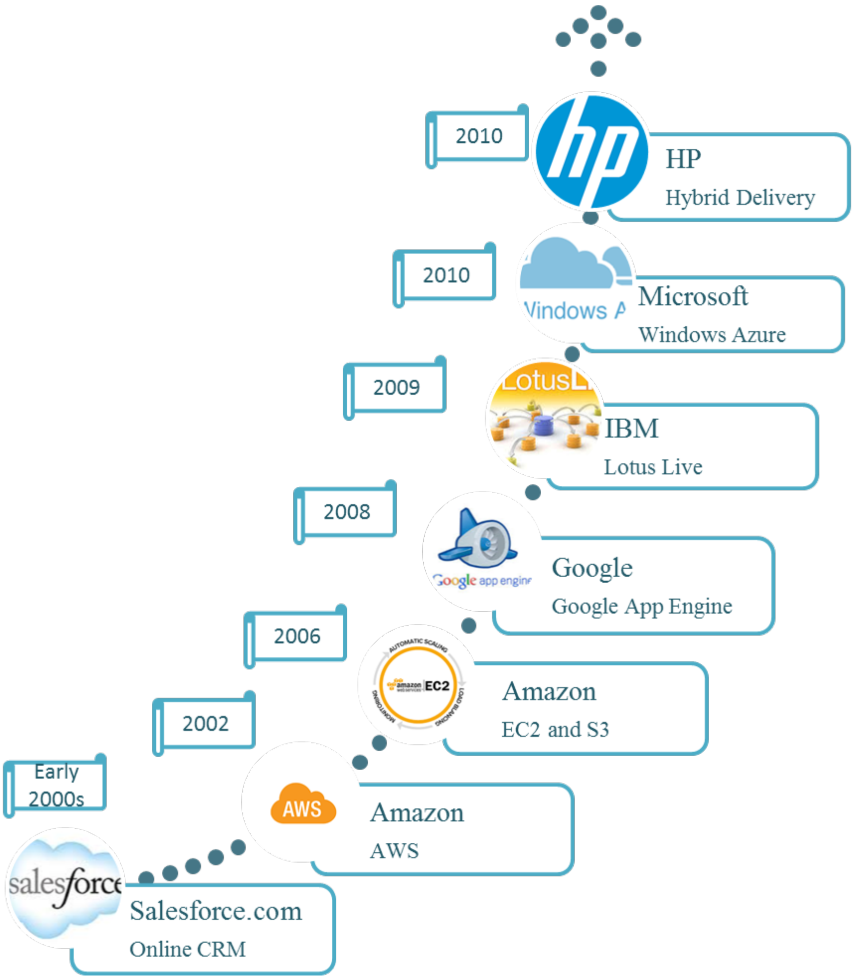


**Figure 8: Evolution of the Cloud Computing market – Based on Su (2011)**

# II. What is Cloud Computing?

## 1. Cloud Computing Definition

Cloud computing is numerously defined by the academic and professional literature. The most widely relied upon technical definition of cloud computing is stated by the US National Institute of Standards and Technology (NIST) where they define CC as "*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of computing resources (e.g., networks, servers, storage, applications, services, etc.) that can be rapidly provisioned with minimal management effort*" (Mell and Grance, 2009, p. 1). Buyya et al. (2009, p. 601) similarly define CC as "*a type of parallel and distributed systems consisting of collection of* *interconnected virtualized computers that are dynamically provisioned and presented as one or more unified computing resource based on service level agreements established through negotiation between provider and customer*". In addition, Venters and Whitley (2012, p.181) define CC as "*a new computing paradigm that allows users to temporarily utilize computing infrastructure over the network, supplied as a service by a cloud provider at possibly one or more levels of abstraction*". Babcock (2010) and Durkee (2010) provide a simplistic definition for cloud computing, stating it is based on outsourced shared-resource computing that is accessed by customers from a large external datacenter and through the use of the internet. On the other hand, the professional literature provides less technical definitions for CC, where Forrester[12] states that CC represents "*standardized IT capabilities (service, software or infrastructure) delivered via internet technologies in a pay-per-use self-service way*" and Gartner[13] defines it as "*a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service to external customers using Internet technologies*". In this research work, we will adopt the definition proposed by the NIST as it represents a holistic and detailed definition of cloud services.

## 2. Cloud Computing Characteristics

Based on the cloud computing definition provided by the NIST, it combines the following five essential characteristics; on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

The on-demand self-service characteristic of CC allows customers to automatically get computing capabilities (network storage, server time, etc.), as needed, and without any human interaction. CC allows a broad network access where customers access capabilities available on the network through standard mechanisms (phones, laptops, tablets, etc.) In addition, CC is characterized by its resource pooling where the providers' resources are "*pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand*" (Mell and Grance, 2009, p. 1). Moreover, CC provides rapidly elastic demand for customers who need to scale

[12] https://www.forrester.com/Cloud-Computing

[13] http://www.gartner.com/newsroom/id/1035013

up and down based on their needs. Additionally, Mell and Grance (2009) state that CC is a measured service where "*cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts)*" (Mell and Grance, 2009, p. 1).

# III. Cloud Ecosystem

## 1. Components of the Ecosystem

An ecosystem represents any system or network of interconnected parts that interact with each other and with their environment. In parallel, a cloud computing ecosystem represents a complex system of interdependent components working together to enable the provision of cloud services. Therefore, a cloud ecosystem encompasses several main actors; Cloud Service Provider(s) (CSPs), Cloud Service Partner(s) (CSNs), Cloud Service User(s) (CSUs), auditors, stakeholders, and regulating bodies (Marston et al., 2011; Schmidt et al., 2015).

Cloud Service Providers are organizations providing and maintaining the delivered cloud solutions, such as software, computing hardware and/or infrastructure services. Cloud Service Partners (CSNs) represent a person or an organization providing support to the building of a CSP service offer. This support includes activities such as service integration, platform migration software, or software monitoring. Cloud Service Users are single users or organizations consuming the delivered cloud solutions. CSPs can also be considered CPUs when they are delivering cloud solutions provided by CSPs to other end users – people, applications, and machines. Auditors represent the external auditors of the CSUs as well as those of the CSPs. Finally, the cloud computing ecosystem includes stakeholders who are numerous parties relying on the external auditors' reports. Regulating bodies, or regulators, represent usually a government body or an international entity. Their role is to penetrate across the previously cited actors. The Internet has become the backbone for transmitting various digital contents, pushing the government to play the role of a mediator. CSPs, CSNs, and other stakeholders will play a vital role in the sustainable adoption of cloud solutions (Marston et al., 2011). Figure 9 shows the relationships and interactions between the different systems in a cloud computing ecosystem.

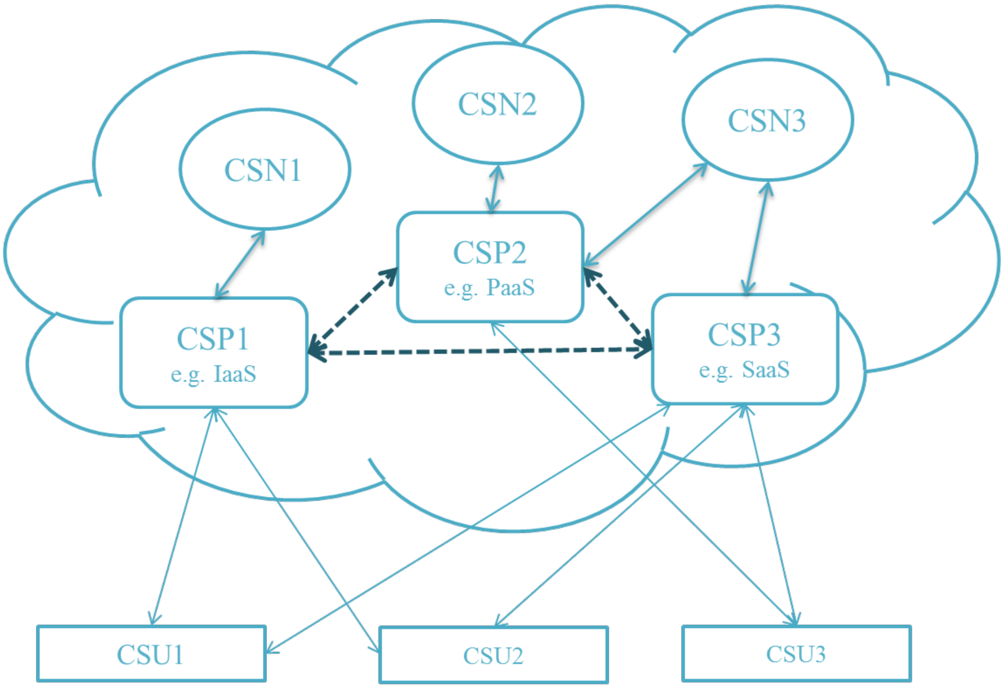


**Figure 9: Cloud ecosystem – Based on ITU (2012)**

The bidirectional arrows in Figure 9 show the two-sided relationship between the different actors in the cloud computing ecosystem. In addition, the dashed bidirectional arrows represent a possible relationship between different CSPs. For example, while CSP1 is getting support from CSN1 in building their service offers, they are providing IaaS cloud services to CSU1 and CSU2. Additionally, CSP1 could be delivering IaaS cloud solutions to CSP2, who is delivering PaaS solutions to CSU3. This emphasizes the possibility of CSPs to also be acting as CSUs.

## 2. Users and Providers Relationship

It is not an easy task for organizations to find the appropriate cloud service providers, from the large list of possibilities. Keeping a good relationship between the organization and the chosen CSPs is really important. Nonetheless, Lacity and Willcocks (2000) identify seven primordial rules to respect, in order to manage the relationship between the organization and its suppliers. They state that organizations should lead a preliminary strategic observation in order to identify its key competences along with the possible outsourced activities. Then, they should evaluate the quality, efficiency and cost of their internal services, in addition to defining the required services and sending them to potential partners. Moreover, organizations should inspect the different offers received from the suppliers and negotiate with them the several contracts clauses. Organizations should, then, manage the transitioning phase while following the execution of the contract (evaluate the different performances, modify some terms, etc.) Finally, they should prepare the (possible) renewal of the contract by continuing with the same supplier, changing suppliers, or integrating some outsourced activities (Lacity and Willcocks, 2000).

# IV. Cloud Service Models

Several cloud services models exist in the literature, however the three most adopted ones refer to a layer of services. These encompass the Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Figure 10 represents the three cloud service models, as well as a few examples of such services. We will take into account these three cloud service models in our research work.


**Figure 10: Cloud service models**

## 1. Infrastructure-as-a-Service

The first layer between the different cloud service models is the IaaS representing the foundation of the cloud environment. A Cloud service provider offers storage, processing and communication through virtual machines. A customer is able to deploy and run arbitrary software, such as operating systems and applications, where they only control the operating systems, the applications, the storage, as well as a few networking components. In this model, the CSPs manage as well as control the underlying cloud environment. However, as shown in Figure 11 cloud service customers only control their virtual machines (Mell and Grance, 2009).

### 2. Platform-as-a-Service

The PaaS is situated above the IaaS layer and represents the integration part of the cloud environment. Cloud service providers in the PaaS model supply the software development tools as well as the programming languages, whereas cloud service users develop their own software. The customer is able to deploy acquired applications on the cloud infrastructure that are created through programming languages and tools maintained by the CSP. Unlike the IaaS model, cloud service users cannot control the underlying cloud infrastructure. They can only control the deployed applications (as shown in Figure 11).

### 3. Software-as-a-Service

The third layer above the PaaS is the SaaS layer, which is the application part of the cloud environment. In this model, cloud service users access their data stored in the underlying cloud infrastructure using numerous client devices through a client interface such as a web browser. Here, cloud service users only control their data, including updates and maintenance.

Figure 11 summarizes the various layers monitored by CSPs and the ones by CSUs, according to the different cloud service models.

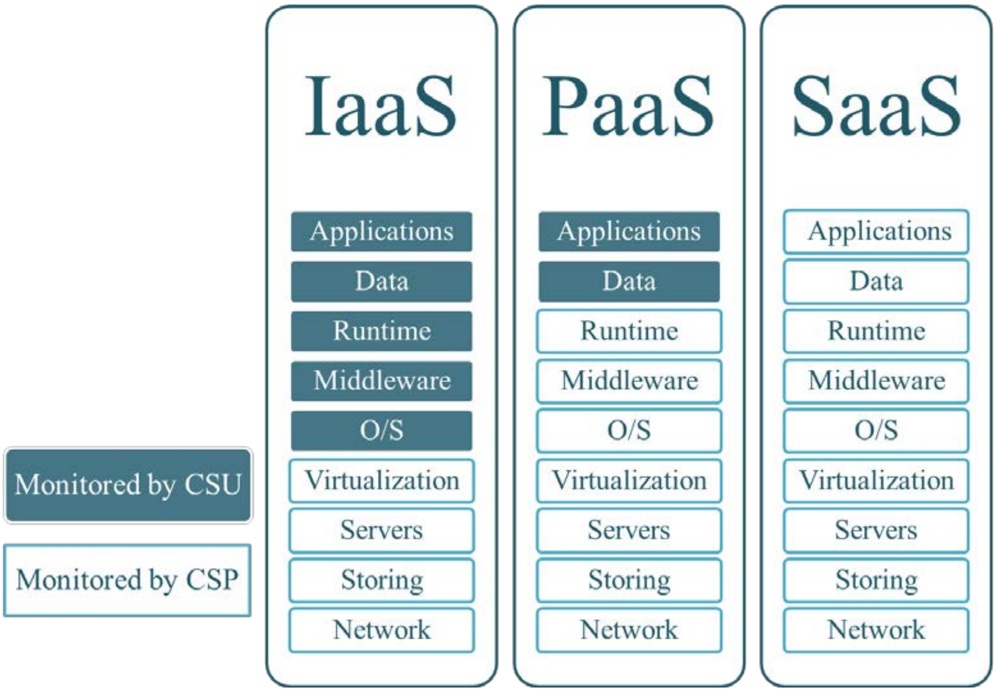


**Figure 11: Monitoring the different cloud service models**

Figure 12, Figure 13, and Figure 14 respectively show examples of SaaS, PaaS, and IaaS cloud solutions. For instance, SaaS services can be used for human resources, social networks, and financial purposes. On the other hand, PaaS users adopt cloud services to develop, test, and deploy applications. Additionally, IaaS services are implemented to host, compute, backup data, for example.

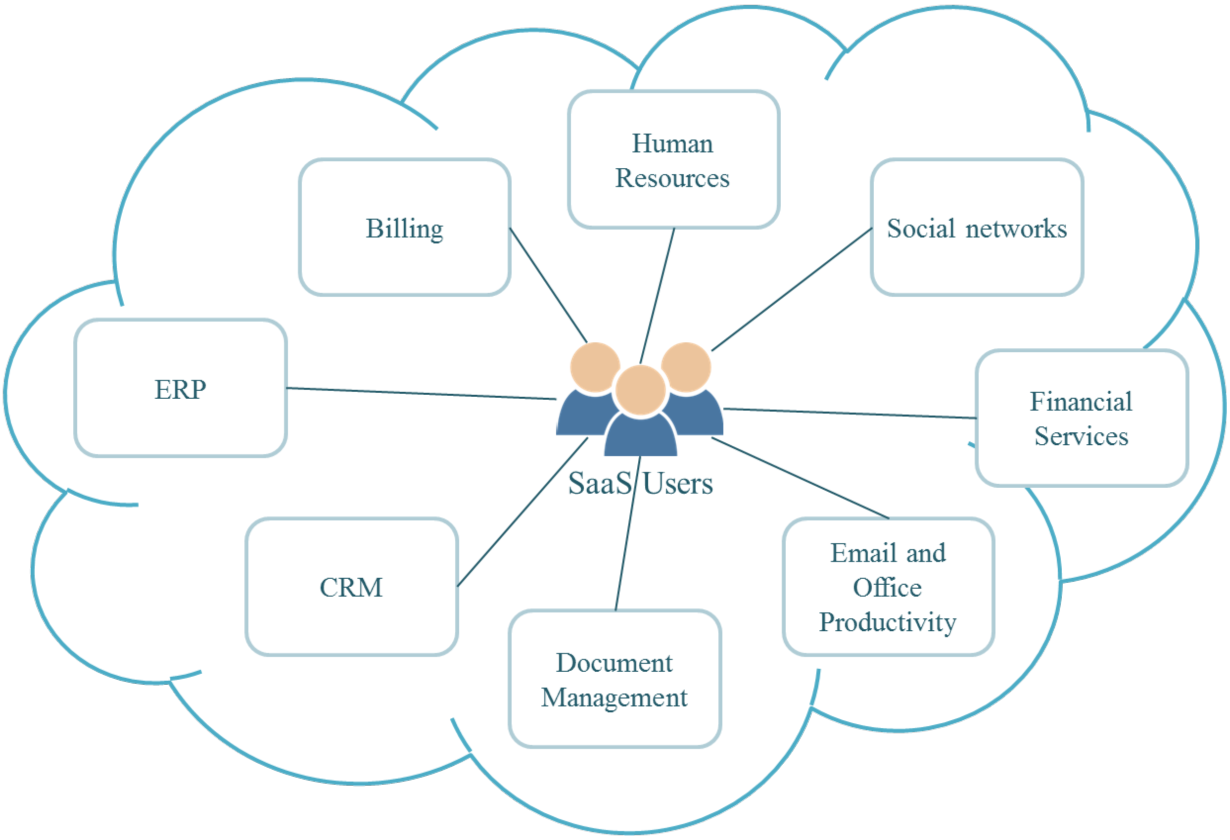


**Figure 12: SaaS examples**

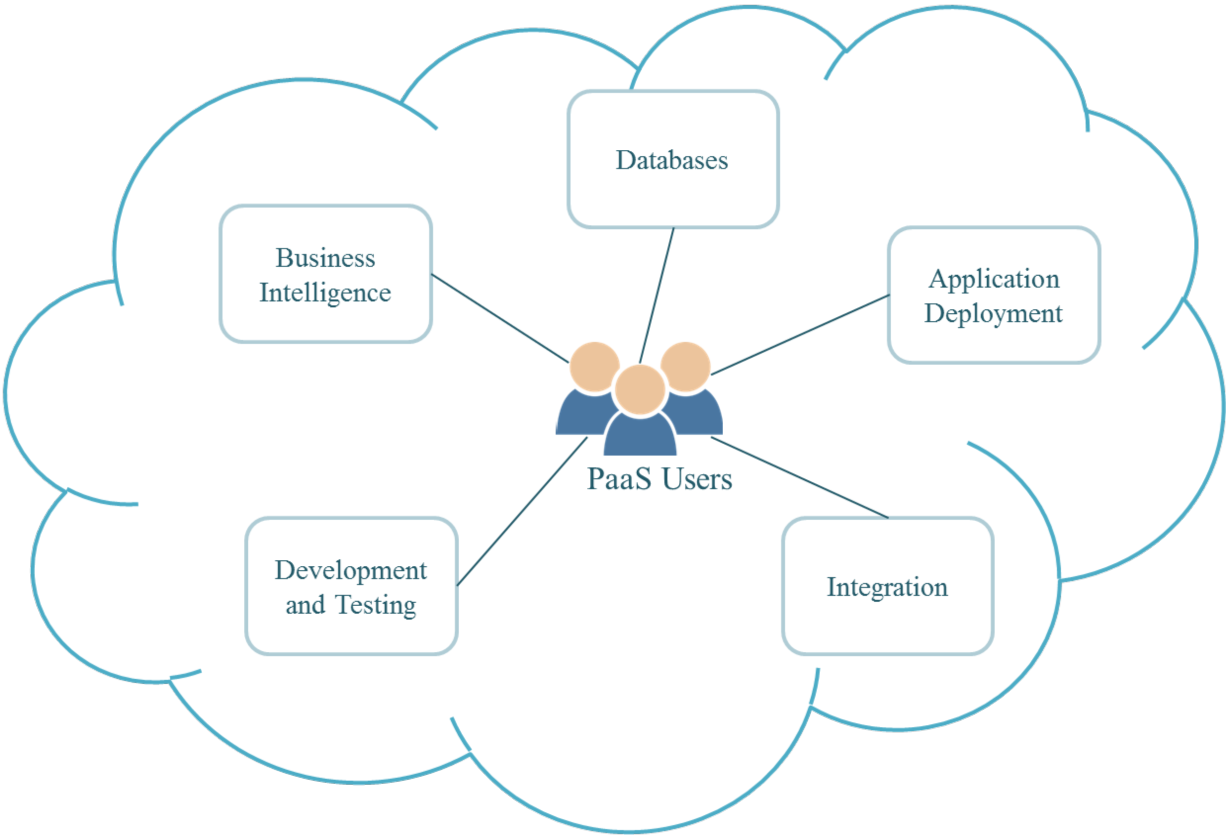


**Figure 13: PaaS examples**

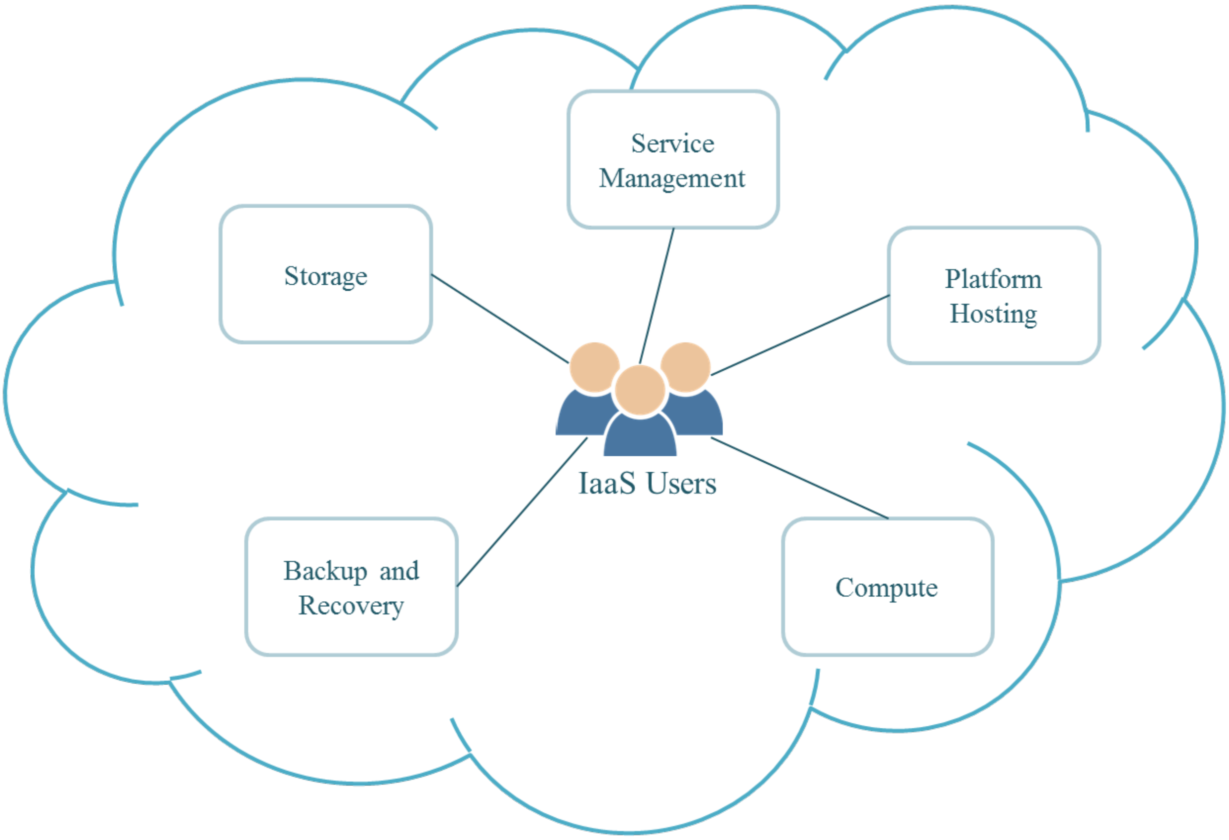


**Figure 14: IaaS examples**

## 4. Cloud Services Examples

The cloud computing market is dominated by various Over-the-Top organizations in different computing areas. For instance, Amazon, EMC, AT&T represent high profile organizations in providing storage and raw computing services. While Cisco, Rightscale and VMWare are involved in offering platform services for organizations, Google, Salesforce, Microsoft and SAP provide software applications. Table 6 shows examples of cloud services according to some high profile cloud service providers. On the other hand, Deloitte, Accenture and IBM are the most triggered organizations for helping others in deploying cloud services.

**Table 6: Examples of cloud services**

| **Service model** | **Providers** | **Services** |
|---|---|---|
| IaaS | Amazon | Amazon EC2 |
| | Google | Google Compute Engine |
| PaaS | Google | Google Application Engine |
| | Microsoft | Microsoft Azure |
| | SalesForce | Force.com |
| SaaS | SalesForce | SalesForce.com |
| | Google | Google Apps |
| | Microsoft | Microsoft Office 365 |

## 5. Cloud Deployment Models

Cloud services can exist under four deployment models; public, private, community, or hybrid clouds. According to Mell and Grance (2009), the NIST states that the infrastructure of a public cloud is provisioned for open use by the public. It is owned and managed by a particular organization (business, academics, government) who also hosts the service, on its premises. The most popular cloud solutions are provisioned from a public cloud infrastructure (Figure 15). The NIST, then, defines the infrastructure of a private cloud to be provisioned for exclusive use by one organization comprising multiple users (multiple business units, for example). It is owned and managed by the organization itself, or a third party or even a combination of the two, existing on or off the premises (Mell and Grance, 2009). Regarding the third deployment model, NIST defines the infrastructure of a community cloud as infrastructures provisioned by a specific community of users from organizations having shared concerns, for an exclusive use. It is owned and managed by one or more organizations from the community, a third party or even a combination of the two, and existing on or off the organization's premises (Mell and Grance, 2009). Finally, the infrastructure of hybrid cloud is a combination of two or more clouds (private or public). They remain bound together by standardized technology that enables data and application portability (Mell and Grance, 2009). Figure 15 illustrates the different deployment services for cloud computing.

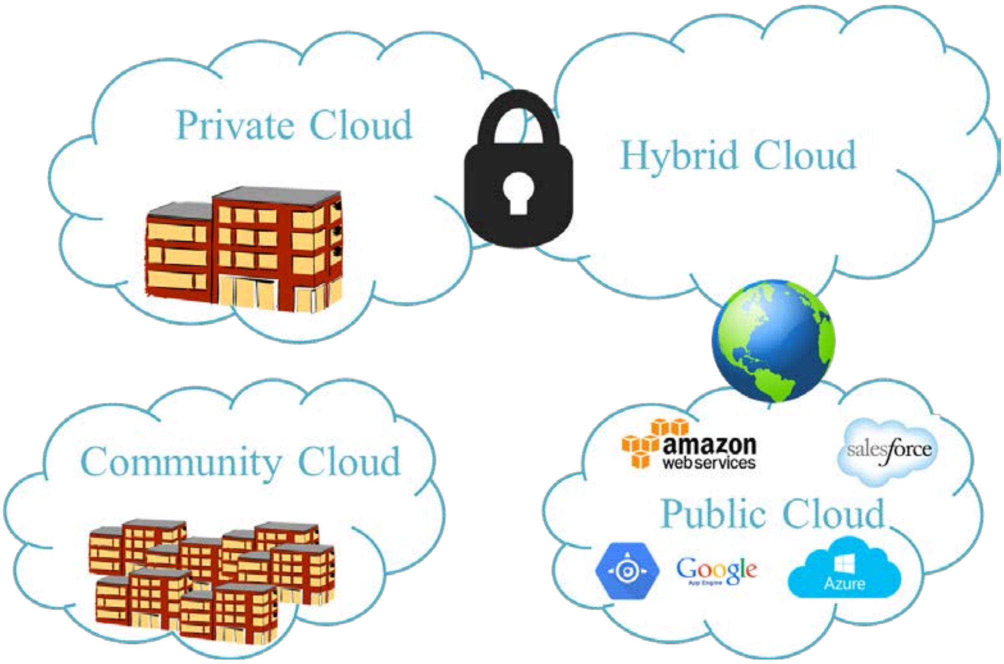


**Figure 15: Cloud deployment models**

## V. Cloud Computing Statistics

Cloud computing has been ranked between the top priorities of businesses throughout the past years. In his study, Brousell (2011) argues that CIOs are shifting from traditional IT approaches to cloud solutions. Morgan Stanley suggests that the compound annual growth for public cloud solutions will be of 50% (Holt et al., 2011). In addition, cloud computing was ranked as a 2$^{nd}$ and 3$^{rd}$ top technology development in 2011 and 2012, respectively (Luftman and Zadeh, 2011; Luftman et al., 2012). The following year Gartner affirmed that CC is rapidly growing and ranking as a top emerging technology in their Gartner Magic Quadrant chart (Gartner, 2013). Moreover, in a large survey involving 276 US IT executives, CC was ranked as a top 3 most significant IT investments by these IT executives, where 81% of them deployed cloud services (Brown, 2013). In 2016, cloud computing remains a top priority for CIOs as mentioned in the Gartner survey[14]. Therefore, as noticed in these previous studies and surveys, cloud service usages are increasing and they are still ranking between the top 3 most important technologies.

In addition to being a top priority, cloud technologies are a top investment for organizations. For instance, Amazon's revenues from providing cloud services to its customers were estimated to be between $500 million and $700 million in 2010 ("Tanks in the Cloud", 2010). Moreover, investments in the cloud are increasing according to Gartner. They forecast that SaaS sales will reach more than $132 billion in 2020 while the IaaS and PaaS sales will reach more than $55 billion (ITA, 2016). They add that, in 2020, the corporate "no cloud" policy will be as rare as today's "no Internet" policy (Gartner, 2016).

# VI. Traditional Outsourcing vs Cloud Computing

## 1. IT Outsourcing vs Cloud Computing

The differences between IT outsourcing and cloud computing are not quite apparent. Nonetheless, in the IS literature, various authors agree on stating main different points between outsourcing IT services and implementing cloud services. While IT outsourcing and cloud computing represent moving in-house resources to an external provider, cloud computing offers a larger number of possibilities and combinations of providers than traditional IT outsourcing. Furthermore, even if users and providers exist in both ecosystems, the length of the contracts between the users and the providers is shorter for cloud services, where cloud contracts offer short lifecycles that can be yearly, monthly, weekly, or even hourly (Leimeister et al., 2010). Therefore, for organizations, implementing cloud services seems more flexible than outsourcing their IT services. Furthermore, Application Service Provisioning (ASP) is a form of IT outsourcing "*where firms rent package software and associated services from a third party*" (Bennet and Timbrell, 2000, p. 196). While ASP and SaaS share similar characteristics, (such as the pricing models and technical aspects), a few researchers argue that ASP led to the emergence of SaaS solutions (Heart, 2000; Benlian and Hess, 2011). Additionally, the elastic characteristic of cloud computing allows organizations

[14] https://www.linkedin.com/pulse/gartner-cios-top-10-technology-priorities-2016-luke-scott

to scale up and down their level of services as needed. Finally, as mentioned earlier cloud services are standardized while IT outsourcing services tend to be more customized. Consequently, even though the concept of IT outsourcing and cloud computing is related to outsourcing IT services, they differ on various points.

### 2. Traditional Datacenters vs Cloud Services

Before the emergence of cloud services, organizations either possessed their own datacenters or outsourced from IT service providers. There are several differences between traditional datacenters and deploying cloud services. For instance, an organization owning a traditional datacenter leads to having full control over the data, customized services, and security (Leimester et al., 2010). Additionally, the organization would benefit from its own economies of scale. However, the organization is limited with its datacenter capacity; hence unless the organization decides to build another datacenter, employees can only use the available capacity.

On the other hand, deploying cloud solutions leads to different characteristics. First of all, the organization is skeptical about the cloud services security since the organization does it via the cloud (the Internet) instead of deploying such services via their local network. Nevertheless, even if the organization does not control its data, it can benefit from economies of scale from the cloud computing ecosystem. Finally, while cloud services are shared among various customers, organizations benefit from a nearly unlimited capacity.

## VII. Cloud Computing a fifth utility?

It is hard to imagine today, a life without having any water – to drink, shower and wash things – electricity – to use appliances in the presence of lights – gas – to stay warm – and telephony – to stay in contact. With the whole excitement about the emergence of cloud computing, opinions are opposed on whether it will be considered as a fifth utility after water, electricity, gas and telephony. Buyya et al. (2008) declare that computing, in general, is being converted to a model consisting of services that are commoditized and delivered similarly as traditional utilities. Lasica (2009) shows the comparison between the migration of cloud computing from soft and hard functions to an off premises service industry, and the migration of electricity in 1900 from location generations to electric grids. Lasica continues with affirming that cloud computing has become people’s entertainment network (YouTube, Flickr, etc.), social network (FaceBook, MySpace, Hi5, etc.), virtual library (Google, Yahoo, etc.), workbench (Picnik, Basecamp, Pando, etc.) and development network (sourceforge.net). In addition, during a roundtable at the Aspen Institute, William T. Coleman III, founder of Cassatt Corporation, predicts that cloud computing will be the platform for the web just like the telephone system has been the platform for voice communication. He also affirms, "*We are about where we were with the automobile, electrical power and radio in the 1910s and 1920s, where all we knew was what they were, but we were just beginning to understand what that meant to improve our quality of life in the future*" (Lasica, 2009, p.9). ISACA (2009) also agrees that cloud computing is revolutionizing the IT services by making computing a universal utility; organizations have now the option to pay for the IT services they use just as they pay for consumed electricity, water, gas and telephony. In addition, after listing the various cloud advantages, Vishwakarma (2012) states that it would become a fifth utility, whose role is to meet people's everyday needs. He adds that it is due to the latest advancement of Information and Communications Technology (ICT) for the past decades that cloud computing is perceived to be essential for the future.

On the other hand, Brynjolfsson et al. (2010) are against the idea of nominating cloud computing as a fifth utility. They discuss that even if businesses rely on electricity just like they rely on IT, they do not need a highly experienced staff to deal with electricity unlike IT. They argue that cloud computing cannot be considered a utility, because if it were one, its challenges would have been solved similarly to the other utilities. They also add that as long as the innovation continues at such a fast pace, cloud computing could not be dealt with as a utility. Therefore, opinions are still contradicting on whether cloud computing will become people's basic necessity: demanding computing solutions in order to fulfill their needs.

## VIII. Cloud Computing Benefits vs Risks

The emergence of cloud computing as a new computing paradigm led to a large academic literature studying its benefits along with its risks.

### 1. Cloud Computing Benefits

Starting with the cloud computing benefits, most literature cites the cloud's economic benefits stemming from economies of scale in providing IT services from large datacenters (Armbrust et al., 2010; Chebrolu, 2011; Kundra, 2011), low maintenance fees (Dutta et al., 2013; Sultan, 2011), and lower needs of functional staff and in-house expertise (Yeboah-Boateng and Essandoh, 2014; Zhang et al., 2010). The pay-per-use characteristic of cloud technology allows users to pay for the consumed amount of computing resources (Onwubiko, 2010; Wei et al., 2009). CC offers organizations cost-effective solutions that allow them to switch their capital expenditures (CAPEX) with operational expenditures (OPEX) (Marston et al., 2011; Zhang et al., 2010). In addition to its economic benefits, cloud technology is also considered a green computing alternative, as it requires less hardware on-premises, supports lower carbon emission, and requires lower electricity consumption (Dutta et al., 2013; Yeboah-Boateng and Essandoh, 2014). Cloud services provide an affordable entrance and access to IT for SMEs and start-ups that cannot afford large hardware fees (Marston et al., 2011; Srinivasan, 2013) as well as for organizations in less developed countries (Marston et al., 2011).

As mentioned by several researchers, CC is highly scalable. This flexibility allows organizations to allocate computing resources on demand (Benlian and Hess, 2011; Chebrolu, 2011; Onwubiko, 2010), and dynamically scale up or down with minimal interaction with cloud service providers (Armbrust et al., 2010; Marston et al., 2011). Some authors argue that through a good quality of cloud services (Buyya et al., 2009), robust virtual machines (Vishwakarma, 2012), and simplified operations (Rajendran, 2013), the organization's performance is increased. In addition, while cloud computing supports the digitization of business processes, it can lead to different forms of innovation, as argued by Kundra (2011), Marston et al. (2011) and Yeboah-Boateng and Essandoh (2014). It enables new classes of applications (such as mobile applications, parallel batch processing, business analytics, IoT, etc.) (Kundra, 2011), it lowers the IT entry barriers (Marston et al., 2011), and spurs the creation of new start-ups and markets (Yeboah-Boateng and Essandoh, 2014).

Researchers are also starting to discuss how cloud solutions can lead to more organizational agility (Garrison et al., 2012; He, 2011; Rajendran, 2013). Some argue that processes can become more agile, departments work together and communicate more effectively through the adoption of cloud services (Yeboah-Boateng and Essandoh, 2014), and projects have a lower time-to-market (Chebrolu, 2011). Furthermore, cloud computing increases utilization of IT resources, both in terms of increasing end use (Marston et al., 2011) as well as increasing the utilization of computing capacity through resource virtualization (Armbrust et al., 2010). Finally, Buyya et al. (2009), Onwubiko (2010) and Rajendran, (2013) state that the ubiquitous characteristics of cloud computing make it more attractive, as users are able to access their data anywhere they are located, anytime they desire, and via any device they possess. A summary of the different cloud benefits found in the literature is displayed in Table 7.

**Table 7: Cloud Computing benefits**

| **Category** | **Benefits** |
|---|---|
| Economics | - Economies of scale for providers (e.g. Onwubiko, 2010; Srinivasan, 2013)<br>- Reduced training costs (e.g .Zhang et al., 2010; Yeboah-Boateng and Essandoh, 2014)<br>- Low price (e.g. Armbrust et al., 2010; Benlian and Hess, 2011; Zhang et al., 2010)<br>- Shifting CAPEX to OPEX (e.g. Onwubiko, 2010; Wei et al., 2009)<br>- Lower electricity consumption (e.g. Dutta et al., 2013; Yeboah-Boateng and Essandoh, 2014)<br>- Easy entrance for developing countries (e.g. Marston et al., 2011; Goundar, 2010)<br>- Easy entrance for start-ups and SMEs (e.g. Srinivasan, 2013; Yeboah-Boateng and Essandoh, 2014) |
| Scalability | - Computing resources on demand (e.g. Buyya et al., 2009; Tiers et al., 2014)<br>- Scale up and down dynamically (e.g. Joha and Janssen, 2012; Onwubiko, 2010)<br>- Minimal interaction with CSPs (e.g. Brynjolfsson et al., 2010; Rajendran, 2013) |
| Performance | - Good quality of services (e.g. Benlian and Hess, 2011; Dutta et al., 2013; Vishwakarma, 2012)<br>- Simplified operations (e.g. Armbrust et al., 2010; Rajendran, 2013)<br>- Robust machines and services offered (e.g. Buyya et al., 2009; Vishwakarma, 2012) |
| Innovation | - New applications and services (e.g. Kundra, 2011; Marston et al., 2011)<br>- Lower IT barriers to innovation (e.g. Kundra, 2011; Marston et al., 2011)<br>- New markets (e.g. Brynjolfsson et al., 2010; Srinivasan, 2013) |
| Agility | - More agile processes (e.g. Kundra, 2011; Rajendran, 2013)<br>- Time-to-market (e.g. Chebrolu, 2011; Yeboah-Boateng and Essandoh, 2014) |
| Utilization | - Easy access for users (e.g. Rajendran, 2013; Zhang et al., 2010)<br>- Optimized resource utilization (e.g. Chebrolu, 2011; Joha and Janssen, 2012) |
| Ubiquity | - Ubiquitous access data and service: anywhere, anytime, anyway (e.g. Vishwakarma, 2012; Zhang et al., 2010) |

## 2. Cloud Computing Risks

The academic literature also identifies several risks associated with CC. Researchers mostly cite privacy and security issues, where managers feel insecure due to possible insider and outsider cyberattacks (Srinivasan, 2013; Sultan, 2011). Hence, storing delicate and private data in a cloud environment is an important issue for organizations (Jaeger et al., 2008; Oredo and Njihia, 2014; Voorsluys et al., 2011). This pushes them to protect their data from such attacks and from simply being lost in the cloud (Armbrust et al., 2010). Various authors also claim that locating data in a cloud environment brings about compliance issues where data should abide by national and supranational laws and regulations such as the Sarbanes-Oxley Act[15] (SOX), the Health Insurance Portability and Accountability Act[16] (HIPAA), or the Cloud Service Level Agreement Standardisation Guidelines[17] issued by the EU Commission (Dutta et al., 2013; Jaeger et al., 2008; Srinivasan, 2013). The moment organizations store their data in another country, thus abiding to the country's respective laws, they witness regulatory ambiguities (Jaeger et al., 2008; Kim, 2009).

Furthermore, as CC enters organizations as a new technology, authors notice integration issues referring to the cultural resistance and technical transition of applications and processes to a cloud environment (Oredo and Njihia, 2014), indicating that not all existing applications will be equally suitable to be migrated to the cloud. A larger number of authors mention that cloud solutions are standardized, limiting the scope for organizations to differentiate from each other (Chebrolu, 2011; Oredo and Njihia, 2014; Rajendran, 2013). Therefore, this lack of customization possibilities of CC affects competitiveness, as noted by Oredo and Njihia (2014). Other authors argue that cloud services are not really reliable (Sultan, 2011; Voorsluys et al., 2011). These authors put forward that cloud servers are unpredictable (Voorsluys et al., 2011), often unavailable (Kim, 2009), and congested (Sultan, 2011) with data transfer bottlenecks (Armbrust et al., 2010). CC is also susceptible to technical failures from poor broadband connectivity as well as bugs in large distributed systems (Armbrust et al., 2010), both resulting in malfunction and downtimes (Srinivasan, 2013). Kim (2009) affirms that such failures are more likely when subscribing to cloud services from untrusted providers.

---

[15] a United States federal law aiming to improve the accuracy and reliability of corporate disclosure in order to protect investors https://www.sec.gov/about/laws/soa2002.pdf

[16] http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx

[17] https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines

According to Dutta et al. (2013), a vital issue when dealing with cloud services is reversibility, referring to both contractual and technical reversibility. Contractual reversibility consists of the lack of a reversibility clause in the signed contracts between users and their CSPs, which can lead to issues when users wish to retrieve their data or transfer them to another CSP (Dutta et al., 2013; Garrison et al., 2012; Oredo and Njihia, 2014). Technical reversibility refers to vendor lock-in situations due to the lack of interoperability and data retrieval (Chebrolu, 2011; Oredo and Njihia, 2014; Voorsluys et al., 2011). Both forms of reversibility limit the freedom to switch from one CSP to another.

The lack of skills was listed as a top issue in a recent survey of cloud computing challenges (Wiens and Ullrich, 2016). With the emergence of cloud services, organizations require new expertise and competences, and thus adequate trainings in order to understand the functionality of adopted cloud solutions and underlying technologies (Rajendran, 2013; Dutta et al., 2013; Oredo and Njihia, 2014). Finally, some researchers highlight that deploying cloud technology is not sufficiently transparent (Dutta et al., 2013; Srinivasan, 2013), as there are hidden costs that users discover only at a later stage. Table 8 summarizes the list of risks found in the recent academic literature.

**Table 8: Cloud Computing risks**

| **Category** | **Risks** |
|---|---|
| **Security** | - Confidentiality of data hinders cloud (e.g. Chebrolu, 2011; Kalyvas et al., 2013)<br>- Sensitive data not suitable for cloud (e.g. Garrison et al., 2012; Noor et al., 2013)<br>- Insider and outsider attacks (e.g. Dutta et al., 2013; Kim, 2009)<br>- Potential data loss (e.g. Armbrust et al., 2010; Kalyvas et al., 2013) |
| **Compliance** | - Regulations and integrity to laws (e.g. Kim, 2009; Noor et al., 2013)<br>- Location of data critical (e.g. Srinivasan, 2013; Sultan, 2011) |
| **Integration** | - Cultural resistance to change (e.g. Oredo and Njihia, 2014)<br>- Integrating new apps (e.g. Mather et al. 2009; Stanoevska-Slabeva and Wozniak, 2010)<br>- Unsuitability for migrating some existing applications (e.g. Oredo and Njihia, 2014) |
| **Standardization** | - Limited customization (e.g. Stanoevska-Slabeva and Wozniak, 2010; Rajendran 2013)<br>- Competitiveness affected (e.g. Oredo and Njihia, 2014) |
| **Reliability** | - Availability of servers(e.g. Dutta et al., 2013; Voorsluys et al., 2011)<br>- Offers from untrusted providers (e.g. Buyya et al., 2009; Kim, 2009)<br>- Congestion (e.g. Sultan, 2011)<br>- Unpredictability (e.g. Jaeger et al., 2008; Srinivasan, 2013)<br>- Bugs in large distributed systems (e.g. Armbrust et al., 2010; Kim, |

| | |
|---|---|
| | 2009)<br>- Downtime (e.g. Srinivasan, 2013; Sultan, 2011)<br>- Poor broadband connectivity (e.g. Armbrust et al., 2010)<br>- Data transfer bottlenecks (e.g. Armbrust et al., 2010) |
| **Reversibility** | - Contractual reversibility (e.g. Garrison et al., 2012; Sultan, 2011)<br>- Technical reversibility (e.g. Kalyvas et al., 2013) |
| **Skills** | - Lack of competences and training (e.g. Dutta et al., 2013; Kim, 2009)<br>- Not understanding how to use cloud technologies (e.g. Rajendran, 2013) |
| **Non-transparency** | - Hidden costs (e.g. Dutta et al., 2013; Srinivasan, 2013)<br>- Lack of competences and training (e.g. Dutta et al., 2013; Kim, 2009) |

# IX. Cloud Computing Contracts

## 1. Standardized Contracts

Cloud computing contracts bind cloud service providers with their clients. These contracts are primordial when adopting cloud services, even when some services are free. Cloud solutions are available in a large amount and variety in today's market, and are evolving at an extremely fast rate. However, cloud computing contracts are not following the same fast steps. Therefore, CSPs tend to offer standardized and uniform contracts for their clients, whether they are providing IaaS, PaaS or SaaS cloud services. Applying a uniform contract for cloud services is beneficial for both parties; the CSPs and the clients. On the first side, while uniform cloud contracts are compatible with the predominant laws, they help CSPs avoid complicated issues. CSPs will particularly avoid facing court issues had the contracts lacked pertinence. Furthermore, this uniformity pushes CSPs to provide better services for clients and hence compete better. Their aim will be focused on keeping their clients satisfied with better marketing services (Silalahi, 2011). On the other side, the uniformity of cloud contracts will also benefit clients where they will feel safer agreeing on a contract signed by others. Consequently, clients will evaluate CSPs based on their quality of service and reputations.

When Over-the-Top CSPs reign over the cloud computing market, contracts become non-negotiable. It is important to notice that only a few exceptions exist when the client is a governmental institution or a wealthy organization ready to pay large amount of money to customize their contract.

## 2. List of Possible Clauses

Uniform cloud computing contracts usually possess numerous clauses. According to the literature, the following clauses are prone to exist in a uniform contract (Hon et al., 2012; Bradshaw et al., 2011, Silalahi, 2008).
The liability clause describes the limits, exclusion, and remedies, when guarantees are breached, along with the possible indemnities. In addition, the resilience, availability, performance and Service Levels clause encompasses different subjects, including the data integrity, resilience of the organization and its continuity, the agreed upon service levels along with the service credits, and the transparency of the providers. A vital clause for most organization is the confidentiality and the right to monitor, access and use clients' data. In addition, regulatory issues are important, stating the location of the data, its processor agreements, and its subject rights. The security rights and breaches clause includes audits, audit rights, security policy, pre-contractual penetrating testing, incident responses, and certification. Another clause states the lock-in issue of cloud computing, explaining the data deletion and portability. The term and termination clause is also important as it presents the minimum terms of the contract, its renewals, and its notice periods. Another clause describes the reversibility issues faced when contracts are breached by one of the two parties. It explains the steps after a breach occurs and states whether the programming language used for the clients data are effective on other platforms. This clause is mostly important for IaaS or PaaS cloud solutions, where SaaS solutions deal with software services, leaving the clients' data intact. Cloud computing contracts also include Intellectual Property Rights and changing service description.

These clauses are either presented to the clients in the form of one whole document or several documents.

## 3. Contracts Documents

Creating cloud computing contracts is a vital step in the life of cloud solutions. The entire cloud computing ecosystem will benefit from building a contract to apply on cloud solutions. On one side it assures clients who will feel safer and more protected when adopting cloud services, and on the other side, the likelihood of facing legal issues in courts will decrease.

Before organizations buy cloud services, they meet with the CSPs in order to discuss the contract of the chosen services. Several types of cloud computing contracts exist. When CSPs offer several cloud contract documents to their clients, these regroup the Term of Service (ToS), Service Level Agreements (SLAs), the Acceptable Use Policy (AUP), and the Privacy Policy (PP).

These contract documents dictate clauses related to the different aspects that need to be agreed upon by the client and their CSPs. For instance, the ToS describes important provisions while encompassing clauses regarding the Intellectual Property Rights, cloud services scope, the applicable laws to the contract and to its termination, the data stored in cloud services, as well as the different client and provider obligations. For example, Amazon Web Services (AWS) states in their clause of *Disclaimer of Warranties and Limitation of Liability* that "*If you use the AWS Site, you are responsible for maintaining the confidentiality of your AWS account and password and for restricting access to your computer, and you agree to accept responsibility for all activities that occur under your account or password"*[18]. Dropbox stresses on the importance of the security of their clients' data "*Everything you store on Dropbox is encrypted both in transmission and storage. Nobody can access your files unless you choose to share them yourself"*[19] (Bradshaw et al., 2011).

In addition, SLAs are extremely important as they state the expected level of services offered by CSPs. Along with the level of service, this document specifies the level of customer support and penalties when cloud services have a longer downtime than agreed upon. As clients rely on a third party to fulfill their needs, it is extremely important that this third party offers highly reliable services. Several downtime incidents have pushed clients to be aware of the possible unreliability of cloud services, such as the service outage of Amazon S3 on February 15, 2008 that lasted nearly two hours (Jaeger et al., 2008). Therefore, the SLA clauses need to be read judiciously. For instance, in the AWS SLA document, they clearly state, "*Neither we nor any of our affiliates or licensors will be responsible for any compensation, reimbursement, or damages arising in connection with: …. (iii) without limiting any obligations under the SLAs, any unanticipated or unscheduled downtime of all or*

[18] Clause of "Disclaimer of Warranties and Limitation of Liability" of ToS. Amazon AWS. Available at: http://aws.amazon.com/terms/

[19] Supra note 48 page 30

*a portion of the services for any reason, including as a result of power outages, system failures or other interruptions ….”*[20] In addition, service client percentage is offered to clients when they do not receive the agreed upon quality of services. Regarding Amazon EC2 and EBS cloud services for example, when eligible, they offer different service credit percentage with respect to the different SLAs; 10% service client percentage when the SLA is between 99.0% and 99.95%, and 30% service credit percentage when the SLA is less than 99.0%. They state "*Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide Amazon EC2 or Amazon EBS is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA*" [21].

Moreover, the AUP describes the laws defining the allowed as well as the prohibited acts of clients when adopting cloud services. This document is based on an ethical behavior and lawful perspective expected from the clients as well as the CSPs. One example of obligations stated in the Directive of the European Parliament and Council's AUP is "*the use of e-mail for direct marketing is only allowed to recipients who have given their prior consent"*[22]. Rackspace, for example, clearly state in their AUP document, "*Rackspace, which prohibits the user to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without expressed authorization of the owner of the system or network"*[23].

Furthermore, the PP includes clauses related to data privacy; particularly, handling the clients' personal information. It also governs the CSPs' behaviors related to their clients' data, such as sharing them with a third party without the clients' agreement. In their Use of Your Personal Information clause, Microsoft states that "*Personal information collected on Microsoft sites and services may be stored and processed in the United States or any other country…"*[24]

---

[20] https://aws.amazon.com/agreement/
[21] https://aws.amazon.com/ec2/sla/
[22] Article 13 of the Directive 2002/58 on Privacy and Electronic Communications. Available at: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32002L0058
[23] Article 1.1 of AUP. Rackspace. Available at: http://www.rackspace.ae/uploads/involve/user_all/64_Acceptableusepolicy.pdf
[24] Clause on "Use of Your Personal Information" of Privacy Statement. Microsoft. Available at: http://privacy.microsoft.com/en-us/fullnotice.mspx

They continued while assuring their clients that they "*will not disclose your personal information outside of Microsoft and its controlled subsidiaries and affiliates without your consent*"[22].

# X. Impact of Cloud Computing on Organizations

## 1. Organizational Transformations

The innovative nature of new technologies yields to several organizational disruptions and encompasses some adjustments or even the whole organizational restructuring (Chatterjee et al., 2002). According to Fitzgerald et al. (2013) and Horlacher and Hess (2016), a digital transformation is driven by new technologies such as Social media, Mobile, Analytics, Cloud, and Internet of Things (IoT). These technologies support major organizational enhancements including, improving customer services, creation of new business models, and streamlining operations (Horlacher and Hess, 2016). Several other researchers claim that cloud computing is a new technology that will engender several changes to the way IT is handled (Carr, 2008; Zhang et al., 2010; Venters and Whitley, 2012). Therefore, implementing new technologies, as cloud solutions, in an organization is not a simple task. While organizations gain significant opportunities of transformations through IT, these generated changes are not safe or easily implemented (Markus, 2004). For instance, Carr (2008) notes that the biggest obstacle of cloud computing will not be technological; however, it will be related to the attitude of the organization towards implementing cloud solutions. Similarly, Marston et al. (2011) state that the emergence of cloud computing will change the corporate IT structure where various intra-organizational issues should be addressed; including the type of cultural change, the way to address this change, and the way to convince employees in accepting this change. As added by Wang and Ramiller (2009), when the organization faces limited know-how, the correct level of adjustment is problematic, especially in the first stages of cloud adoption. Moreover, cloud computing engenders several complications for the corporate and IT governance of the organization. For instance, the decision makers should expand the organization's governance by considering the several additional issues generated by cloud services, including reversibility, vendor lock-in, disaster recovery, shared management, etc. (Hsu, 2012).

Therefore, some argue that establishing policies and standards are extremely imperative in the initial stage of the cloud adoption in order to maintain effective IT governance (Marston et al., 2011; Hsu, 2012). Moreover, implementing a strategy to handle the different issues related to cloud solutions is essential. Researchers recommend organizations, especially large ones, to build their own cloud strategy while ensuring it is aligned with where their business is heading (Marston et al., 2011). Their cloud strategy would be about bringing together all stakeholders in order to interact more efficiently and perceptively as well as to make the best decisions at the lowest possible cost. For instance, Lapon (1999) adds that organizations aiming at adopting new technologies (such as cloud computing), can adopt one of these three strategies; innovation strategy, "wait-and-see" strategy, and "following" strategy. Innovation strategy consists of adopting the new technology in its emergence phase, which maximizes the benefits along with potential risks. The "wait-and-see" strategy is based on prioritizing the security and reduction of costs, hence adopting technologies that are in the maturity phase. Finally, the "following" strategy settles in between these two strategies, where organizations adopt popular technologies yet not on the large scale. However, there's no general rule dictating the choice of one strategy.

Moreover, cloud computing drives organizations to redesign their business processes in order to achieve higher levels of organizational transformations (Battleson et al., 2016). Adopting cloud solutions also pushes organizations to restructure the relationships in their business network which will allow them to leverage competencies owned by partner organizations (Battleson et al., 2016). For instance, the cloud platform facilitates coordination among multiple agencies involved in business processes. Further, cloud computing attracts new customers while creating new services and products. This, hence, redefines the organization's business scope. In addition, as an innovative technology, cloud services lead to architectural changes in IS (Bernstein et al, 2009; Dillon et al, 2010). For instance, changes in the software and hardware in addition to their interconnections make the cloud architecture distinct from other computing models (Battleson et al., 2016). They affirm that adopting cloud solutions in an organization need to be properly governed. This governance would address security control issues, data protection issues as well as compliance with organizational standard issues, in order to monitor and enhance controls over the different organizational processes.

Consequently, the impact of adopting cloud solutions in organizations is highly evoked by researchers in the literature. Organizations should take into considerations all these transformations when studying the transition towards cloud computing.

## 2. Development of New Skills in Organizations

From the many changes engendered by the emergence of cloud computing is the need for new competences and skills. The lack of specific skills is cited as a major CC drawback by several researchers (Rajendran, 2013; Dutta et al., 2013; Kim, 2009: Janssen and Joha, 2011). According to a research conducted by Portio Research in 2009, 56% of the interviewed European CIOs (196 CIOs out of 350) lack the required knowledge or skills to effectively adopt sophisticated cloud solutions (Flechaux, 2009). This lack raises vital governance questions for organizations, specifically the ones aiming at staying competitive.

Therefore, it is imperative for the different employees, especially IT employees, of organizations that are starting to implement cloud solutions to develop a new set of skills and competences. For instance, Morgan and Conboy (2013) raise the presence of a high level of anxiety from IT employees worrying about losing their jobs as their skills become obsolete. They continue by advising organizations to offer training sessions in order to increase their employees' competences. Furthermore, organizations require competences embedded in their IT governance structures in order to ensure the alignment of the business and IT objectives, as well as the leverage of the IT resources (Weill and Ross, 2004). Cloud solutions represent new types of IT resources for organizations. Therefore, they demand new competences and hence, new governance structures to align the business and IT objectives and leverage the cloud promised opportunities (Prasad and Green, 2015). Organizations, which are immersing themselves in cloud solutions, are highly advised to adopt new governance structures in order to manage more efficiently the new risks generated by these solutions (COSO, 2012) and leverage the new benefits associated with the changed environment (Teece, 2007). Moreover, the new features and characteristics of cloud solutions bring new challenges to organizations in terms of contracts as previously mentioned. Therefore, cloud contracts should be meticulously read and analyzed, one term after the other, in order to avoid confusion, misunderstandings and misinterpretations. For instance, the cloud contracts binding Google and the City of Los Angeles showed major data breach issues, since the term "lost data" was not defined with enough details and precision (Info Law Group, 2010).

## 3. Shadow IT

The shadow IT phenomenon has also been referred to in the literature as feral systems (Houghton and Kerr, 2006), un-enacted projects (Buchwald and Urbach, 2012), and feral practices (Thatte et al., 2012). These commonly describe the situation when business users acquire or use IT without required approval or oversight through corporate IT units. The emergence of shadow IT in organizations raises serious questions regarding its causes, its consequences, and required managerial coping strategies (Kopper and Westner, 2016).

From the frequently cited causes for shadow IT practices is the dissatisfaction of the business departments with the services provided by IT units along with their unfulfilled needs and requirements (Behrens and Sedera, 2004; Jones et al., 2004; Boudreau and Robey, 2005; Houghton and Kerr, 2006; Kerr et al., 2007; Huuskonen and Vakkari, 2013; Lyytinen and Newman, 2015, Ahuja and Gallupe, 2015). Moreover, a few authors affirm that the increased IT systems inflexibility, standardization and rigidity led to the emergence of shadow IT activities within large organizations (Houghton and Kerr, 2006). These characteristics inhibit IT departments from providing customized services fulfilling the totality of their business departments' needs.

Another potential cause of the emergence of such activities is capability-based: In today's digital market and society, business employees are developing their own skills in IT. This enables them to implement their own IT solutions acquired from external providers (Behrens and Sedera, 2004; Jones et al., 2004; Spierings et al., 2014; Schalow et al., 2013; Zimmermann and Rentrop, 2014; Ahuja and Gallupe, 2015). The academic literature has identified several other factors influencing the emergence of shadow IT practices, such as independency on the IT department (Zainuddin, 2012), self-determination needs (Ahuja and Gallupe, 2015), and business and IT misalignment (Zimmermann and Rentrop, 2014). Moreover, the emergence of cloud computing has driven the proliferation of shadow IT, as cloud services often demand a minimum IT competences from business users to customize and use them (Schalow et al., 2013; Winkler and Brown, 2014).

Nevertheless, shadow IT activities are generally linked with a number of negative consequences. Most prominently, researchers cite unintended security and privacy issues (Györy et al., 2012; Schalow et al., 2013; Walters, 2013; Kretzer and Maedche, 2014; Walterbusch, 2014). For instance, organizations have witnessed how shadow IT activities lead to disruption of controlled environments (Györy et al., 2012), data loss (Walters, 2013), and non-compliance with organizational security policies (Alter, 2014). While business departments use services not provided by the IT department, shadow IT practices would cause a loss of synergies between the different departments (Györy et al., 2012), and hence lead to the creation of resource conflicts between departments, having each of their own interests (Buchwald and Urbach, 2012). It is important to highlight that employees may not be sensitized to the problems related to shadow IT, thus having a mindset that buying solutions from cloud service providers is not risky (Dittes et al., 2015).

Nonetheless, the academic literature has also stressed on the possible positive consequences that shadow IT can provide for organizations. For instance, some authors have identified an increase in productivity as a positive effect when business departments short-circuit their IT department (Ahuja and Gallupe, 2015; Schalow et al., 2013). Using shadow services, where information is available at a glance, saves employees' time and helps them focus on their jobs (Huuskonen and Vakkar, 2013; Singh, 2015). In addition to increased productivity, several researchers also mention improved business innovation as a positive outcome of shadow activities (Behrens, 2009; Singh, 2015, Kretzer and Maedche, 2014; Walterbusch, 2014). Business innovation can, for example, be manifested in helping personnel adapt to changes in their organizational environment (Singh, 2015; Györy et al., 2012) or in bringing organizational stability and order (Behrens, 2009). Thus, there is a duality where shadow IT can expose organizations to severe threats, while at the same time result in an improvement of organizations' business and IT capabilities.

Researchers have identified various managerial strategies to deal with this phenomenon. To prevent shadow IT, organizations set up governance structures and formal policies aiming at guiding employees across different levels (Walterbusch, 2014; Zimmermann and Rentrop, 2014) and creating awareness (Klesel et al., 2015; Walterbusch, 2014). In order to better identify the unfulfilled needs of business departments, researchers advise organizations to integrate their business stakeholders in the IT decision-making process (Winkler and Brown, 2014; Klesel et al., 2015). Organizations can start by identifying the different shadow IT systems through interviewing, interpreting help desk requests, and conducting technical analyses (Rentrop and Zimmermann, 2012; Zimmermann et al., 2014; Walterbusch, 2014). IT departments can conduct a network traffic analysis in order to monitor the evolution of shadow IT and identify systems with high dependency between business departments and cloud service providers (Fürstenau and Rothe, 2014).

# XI. Governance of Cloud Computing

## 1. New Governance Mechanisms

The literature emphasizes the complex tasks organizations are facing when wishing to move towards CC. Beaudry and Pinsonneault (2005) affirm that when employees witness changes in their habits, their job performance will be impacted while they attempt to cope with these changes. Therefore, in order to change employees' attitudes and simplify their transitions to cloud computing, organizations are advised to implement an organizational structure with well-defined roles for the responsibility of IT management, business processes, and applications as these elements are moved out of the traditional IT environment and into the cloud. It was discussed in the academic literature that the current IT governance (structures, processes, and relational) mechanisms of an organization are not sufficient in order to implement cloud solutions effectively (Marston et al., 2011; Prasad et al., 2014; Joha and Janssen., 2012). Therefore, implementing new mechanisms for CC will help organizations in benefiting from the various cloud services advantages. However, the literature is still modest regarding the different mechanisms that are needed for the adoption of cloud services. Structure mechanisms are mostly addressed; however, without highly mentioning the required processes and relational mechanisms.

Prasad et al. (2014) state that organizations need to have appropriate governance structures and policies. After an extensive study of the literature, they proposed four governance structures. The first modification to the governance structure is the presence of a Chief Cloud Officer. He will help with the coordination of the cloud services technological efforts to guarantee economies of scale and cooperation. In addition, as the adoption of cloud computing expands, there will be a need for building a management structure to govern these services. Hence, it is important to have a Cloud Management Committee within the organization. The third addition to the organizational structure is a Cloud Service Facilitation. It will be the central cloud operational "nervous system" in the organization that is responsible for managing a strong database of cloud suppliers as well as keeping a good control of the cloud services (Prasad et al. 2014). The Cloud Management Committee and Cloud Service Facilitation will split the work; while the first would addresses the "what" questions related to the cloud services, the latter addresses the "how" questions. Finally, a Cloud Relationship Center is needed to manage the relationship between the cloud service providers and the cloud service users. The Cloud Relationship Center must ensure a dynamic and continuous relationship between those two. It will achieve this by monitoring the daily use of cloud services as well as ensure that the set of cloud services policies are maintained. After proposing these four governance structure, Prasad et al. (2014) test the effectiveness of the adoption of these structures among 136 companies in Australia that are either actual cloud service adopters or potential ones. They conclude that all four additions were primordial; however, having a cloud relationship center was imperative. Therefore, the four mentioned governance structures provide a complete management for cloud services, to guarantee its sustained fit to IT needs in the organization. Cloud service providers also benefit from the governance model as it will help them seek new opportunities to develop governance tools for cloud computing. It will also allow them to enhance their capabilities to better suit their consumers' needs.

Moreover, Joha and Janssen (2012) analyze the IT governance framework introduced by Feeny and Willcocks (1998). They also notice that several, more elaborate additions must be made in order to correspond to implementing cloud solutions effectively. They suggest demand and relationship management capabilities to facilitate the dialogue between the business and IT departments and manage the cloud related problems within the different business units. They also recommend capabilities related to data security management, IT network management, cloud procurement, risk and compliance management, contract management (Joha and Janssen, 2012). In addition, this paper clearly shows the differences between the capabilities required for regular IT outsourcing compared to those required for cloud services (Joha and Janssen, 2012). However, these authors do not offer a complete list of the needed governance mechanisms; they only addressed required structures. In addition, their analysis is only based on the public sector.

Further, the literature highlights the role of the CIO in the presence of cloud solutions. For instance, the CIO is no longer capable of working on the digital transformations solely, where "*digital transformations demand different mindsets and skill sets than previous waves of transformative technology*" (Fitzgerald et al., 2013, p. 6). This pushes organizations to adopt new governance structures when implementing cloud solutions. Researchers as well as practitioners evoke the need for new structures, as the CIO cannot work alone for the transformations generated by these solutions (Weill and Woerner, 2013; Chen et al., 2010; Peppard et al., 2011). Researchers emphasize the lack of skills and capabilities of CIOs to be allocated key responsibilities for the digital transformations (Westerman and Well, 2004; Peppard et al., 2011). These conclusions lead to the creation of new governance structures, responsible for the effective adoption of cloud solutions, such as the high emergence of a Chief Digital Officer (CDO). According to summits held in 2015, the CDO was evoked as the fastest-growing C-level position in organizations (CDO Club, 2015; CDO Talent Map, 2014). However, the academic research about the tasks and roles of CDOs is still not well developed. Few researchers, such as Horlacher and Hess (2016) studied the different major tasks and responsibilities of CDOs in four large organizations. They concluded that the CDO does not only need IT knowledge, but developed competences in strategy development, change management, and communication. The key aim of CDOs is increasing the organizations' sales revenue as well as the market share growth. In addition, as noted in Horlacher and Hess' (2016) results, CDOs aim at creating "*a digitally empowered and customer driven company*".

With the emergence of digital transformations, CDOs and CIOs/CTOs possess distinguished responsibilities, whereas the CDO focuses on the strategic and communication features of the transformation, the others remain focused on the technical features (Horlacher and Hess, 2016).

New governance structures are proactively responsible for driving organizations effectively into their digital transformations, as well as new processes and relational mechanisms. However, research work is still modest regarding the different business transformations and mechanisms needed when adopting cloud solutions. Cloud governance is hence very modest in organizations, which makes them not mature enough to benefit fully from the cloud solutions advantages.

## 2. Existing Cloud Governance Models

As mentioned previously, governing cloud solutions through different approaches, including the implementation of new governance mechanisms, is essential. A few researchers became interested in creating a cloud governance model that will allow organizations to implement cloud services effectively. For instance, the Guo et al. (2010) cloud governance model discusses the aspects of cloud governance in general. It is divided into three parts; the policy model, the operational model, and the management model. The policy model of Guo et al. (2010) includes data policies, service policies, and business process management policies. In addition, the operational model comprises authentication, authorization, audit, monitoring, adaptation, and metadata repository. Finally, the management model consists of policy management, security management, service management, and risk management. However, they do not take into consideration the strategic alignment between cloud objectives and business objectives. In addition, they neglect mentioning the adjustments made regarding the different roles, responsibilities, and organizational structures. Nonetheless, taking into consideration the strategic alignment, in addition to the organizational changes is primordial for an effective adaptation of cloud services. On the other hand, He (2011) proposes a lifecycle cloud governance model. His model identifies five areas of interest, including strategic planning, organizational alignment, service lifecycle management, policy management, and SLA management. This model resembles the model proposed by Guo et al. (2010) with some of the outlined areas. Nevertheless, they differ since He (2011) applies a lifecycle approach, where each lifecycle tackles one area of cloud governance. In addition, Hsu (2012) proposes a cloud governance model, which mostly focused on policies, risks and performance. Hsu's model consists on setting up the different policies and principles in order to create a clear governance strategy and management plan. In addition, it focuses on evaluating the risks associated with cloud computing through audit committees. Hsu (2012) states that the CIO plays a very important role in cloud governance through supporting the boards and several committees. Finally, he adds that evaluating the performance of the organization when implementing cloud services is vital. He proposes to achieve this with different process mechanisms including, performance dashboards, balanced scorecards, and business intelligence.

Only a few cloud governance models exist in the literature and they seem insufficient to govern properly cloud solutions in large organizations. The models proposed by Guo et al. (2010) and Hsu (2012) focus on one part of the cloud governance and do not tackle all areas. Regarding the one proposed by He (2011), it covers all the different areas of cloud governance; however, it does not mention the way cloud services can be implemented in any organization. Therefore, a clear governance guiding organizations in implementing cloud services is needed.

However, mature governance models for cloud computing are not very present in the literature. While cloud computing is considered an innovation technology, it is part of an organization's IT. Therefore, we posit that implementing cloud solutions can be governed by adapting the existing IT governance to the necessities demanded by such solutions. As mentioned in previous sections, the literature states that cloud services bring changes to the organization. For instance, various new decisions should be made regarding the implementation of cloud solutions. Plus, the location of decision-making authorities changes with such solutions. And finally, they demand new specific structures, processes and relational mechanisms, including new competencies and skills, new relationship with CSPs, better communications between the business and IT departments. Nevertheless, the literature is still modest regarding the different decision makers and mechanisms needed to govern cloud solutions. Therefore, governing cloud services will follow a similar structure as the IT governance frameworks presented by Weill and Ross (2004), De Haes and Van Grembergen (2004), and Peterson (2004). It is also important for organizations to assess their governance once implemented. Nonetheless, the literature regarding the maturity of cloud solutions is also modest. Therefore, we decided to address the different maturity models present in the literature to be able to assess the maturity of cloud services adoption by organizations.

# Third Section: Maturity Models

## I. Maturity Model Definition

Models represent a description of the environment in order to understand “what” is happening in it (Mettler and Rohner, 2009). Simpson and Weiner (1989) affirm that maturity represents the fact of being in a ready, complete or perfect state. In order to reach the ready state, organizations need to evolve from their actual state – usually an initial Ad Hoc state – to get to the desired or mature state. While maturity models are constituted of various maturity levels of a domain, they help organizations in evolving from one level to the other, reaching the desired outcomes (Lahrmann et al., 2011).

While IT and business managers usually know the challenges they face, they might disagree on which improvements are the most required within their organization. Deploying a maturity model is therefore important in order to achieve a consensus between the IT and business managers.

## II. Existing Maturity Models

Various assessment methods along with standard IT governance frameworks have existed in the literature, aiming at improving organizations’ IT governance and management. From the large list of standard frameworks (ITIL, SAS70, ISO 17799, SysTrust, Prince2, etc.), the most common ones related to maturity are the Control Objectives for Information and related Technology (COBIT), the Capability Maturity Model (CMM), the Capability Maturity Model Integration (CMMI), and the IT Capability Maturity Framework (IT-CMF).

### 1. COBIT Framework®

COBIT represents the Control Objectives for Information and related Technology. This framework has been developed by the ITGI (2000) aiming at achieving good IT security and control practices. The COBIT is a tool used for measuring the organizational performance, providing best practices for IT processes based on a list of critical success factors, and assessing the organization’s maturity. Organizations tend to only use a few features of the COBIT framework, due to its complicated usage.

## 2. Capability Maturity Model®

The Capability Maturity Model (CMM) is a maturity model proposed by the Software Engineering Institute of the U.S Department of Defense. It identifies the maturity level of the organization regarding its processes capabilities. Paulk et al. (1993) state that the CMM focuses on the improvement of processes in the organization, across five levels; the initial level, the repeatable level, the defined level, the managed level and the optimizing level. In the initial level, organizations have *ad hoc* software processes, where only a few of them are defined. The repeatable level is constituted of basic project management processes. It is called the repeatable level because organizations repeat the previously successful process disciplines with new adopted projects. Additionally, software processes are documented and standardized in the defined level. In the managed level, organizations collect detailed measures of the product quality and software processes. Finally, in the optimizing level organizations get a continuous process improvement through a quantitative feedback from innovative technologies and ideas (Paulk et al., 1993). While the CMM is a descriptive model (describes key capabilities normally characterizing an organization at a certain maturity level), Paulk et al. (1993) state that it is not a prescriptive model as it does not state the means required by the organization in order to improve and move from one level to the next one. For instance, while the CMM describes the organization at each of the five maturity levels, it does not prescribe the exact ways to get to each level. Paulk et al. (1993) add that jumping to the next maturity level usually takes around two years.

The Capability Maturity Model Integration (CMMI) is the successor of the CMM. It is also constituted of five maturity levels but instead of addressing processes, the CMMI emphasizes result-oriented processes. While the CMM only considers the completion of a specific activity, the CMMI considers whether the completed activity have achieved the desired results. It is important to note that both models focus on software development projects.

## 3. IT Capability Maturity Framework®

The Innovation value Institute developed the IT Capability Maturity Framework (IT-CMF) (Innovation Value Institute, 2012). It seeks the assessment and enhancement of organizations' maturity through maximizing business value from IT investments. This framework encompasses four capabilities on the macro level, each composed of critical IT processes. It also defines five common maturity levels; initial, basic, intermediate, advanced, and optimizing. The IT-CMF is basically focused on the IT department of the organization.

## 4. Maturity Models Descendants

Several authors propose new maturity models based on the existing ones and related to various areas in the IS domain. This sub-section

Luftman (2000), ITGI (2000), and Van Grembergen and De Haes (2004) propose a maturity model for organizations' strategic alignment, following the COBIT structure. While these authors define their maturity model on a five-level scale, Duffy (2002) defines one on a four-level scale. However, these various models aspire to providing a tool for organizations, in order to manage easily their strategic alignment journey. In order to face the challenges stumbled upon when implementing current IT governance models in the CC environment, Schmidt and Grabski (2015) propose a Cloud Computing Capability Maturity Model broadly based on the COBIT framework. In addition, Simonsson et al. (2010) create a framework for analyzing the correlation between IT governance maturity and IT governance performance. Based on the four IT governance domains (34 processes) introduced by COBIT, they prove the presence of a direct correlation between some IT processes maturity and IT governance performance. For instance, appropriate definitions of the various roles and responsibilities, the cost allocation, and quality management possess the strongest links with the organization IT governance performance (Simonsson et al., 2010).

Similarly, the CMM and CMMI frameworks were used by several authors. For instance, Bate et al. (1995) propose a Capability Maturity Model for systems engineering in order to assess system engineering in organizations based on the present capabilities in these organizations. They define 5 maturity levels regarding systems engineering, which are the performed informally level, the planned and tracked level, the well-defined level, the quantitatively controlled level, and the continuously improving level. Bill et al. (1995) propose a People Capability Maturity Model (P-CMM) also based on the structure of the original CMM (Paulk et al., 1993). The P-CMM focuses on improving the management of human assets in IS organizations. While it is based on the structure of the original CMM, the authors state a five-level maturity model, starting with an initial level, repeatable level, defined level, managed level, and ending with an optimizing level. Similarly, Herbsleb et al. (1997), and Dorfman and Thayer (1997) offer a Capability Maturity Model for the software development area, and

Cooper and Fisher (2002) for the software acquisition area. Niessink et al. (2005) describe the IT service capability maturity model, identifying the different maturity levels for organizations providing IT services (IS operations, mainframes, software system maintenance). They define five maturity levels similar to the original CMM structure; initial level, repeatable level, defined level, managed level, and optimizing level. While Lockamy and McCormack (2004) and Reyes and Giachetti (2010) propose a supply chain Capability Maturity Model, others were interested in building a capability maturity model for project management (Ibbs and Kwak, 2000; Crawford, 2007). In addition, DeBruin and Rosemann (2005) address the assessment of organizations business process management, Kaner and Karni (2004) a capability maturity model for knowledge-based decision making, and Yeo and Ren (2009) a risk management Capability Maturity Model for complex product systems projects. Additionally, Duarte (2013) offers a cloud maturity model based on the CMMI-model (Software Engineering Institute, 2002). It defines various activities helping organizations in migrating their services to the "cloud", assessing the different processes used in the migration, and creating a roadmap to improve these processes. In addition, they use the process improvement approach of the CMMI in order to increase the capability level of the suggested activities by his model (Duarte, 2013). The most vital processes of his model were architecting the cloud contract, engaging the cloud providers, operating the cloud services and regenerating the cloud knowledge. However, Duarte (2013) mainly addresses the processes adopted by the organization during their cloud. This model then only represents one way to tackle the organization's cloud maturity without considering other key factors.

Conway and Curry (2012) propose a cloud maturity model based on the IT-CMF (Innovation Value Institute, 2012). They define the vital processes addressed by the cloud service users before moving their various IT services to cloud services. While Conway and Curry's (2012) framework is based on the IT-CMF, it can only be used by IT departments already adopting the IT-CMF. In addition, this framework only helps organizations in managing their IT services in the public cloud.

Some authors like Kang et al. (2010), only based their research work on case studies in order to build a SaaS maturity model aiming at helping Cloud Service Providers migrate their systems to SaaS platforms. Their model consists of four maturity levels; Ad Hoc, standardization, integration, and virtualization. It addresses four service components, including the data, the system, the service and the business. As Cloud Service Providers mature in the different service components, they will find more facilities in moving their systems to a SaaS platform, and hence in providing SaaS services to organizations.

Nevertheless, these maturity models do not encompass cloud computing specificities and lack vital factors focusing on the appropriate adoption of cloud services. The actual maturity models lack knowledge in the various cloud concepts. Therefore, Open Data Center Alliance proposes a Cloud Maturity Model based on the CMMI addressing cloud computing from various angles and allowing organizations to evaluate the maturity of their cloud adoption. The following section focuses on presenting the maturity model presented by the Open Data Center Alliance, where we argue the reasons for basing our research work on this maturity model.

Table 9 summarizes the different maturity models proposed in the academic and professional literature and based on one of the previously presented models.

**Table 9: Summary of maturity models found in the literature**

| Maturity Models Basis | Maturity Models Purposes | References |
|---|---|---|
| Control Objectives for Information and related Technology (COBIT) | Organizations' strategic alignment | Luftman (2000) |
| | | ITGI (2000) |
| | | Van Grembergen and De Haes (2004) |
| | | Duffy (2002) |
| | Cloud Computing Capability Maturity Model | Schmidt and Grabski (2015) |
| | Correlation between IT governance maturity and IT governance performance | Simonsson et al. (2010) |
| Capability Maturity Model (CMM) | Systems Engineering | Bate et al. (1995) |
| | People Capability Maturity Model | Bill et al. (1995) |
| | Software Development | Herbsleb et al. (1997) |
| | | Dorfman and Thayer (1997) |
| | Software Acquisition | Cooper and Fisher (2002) |
| | IT services | Niessink et al. (2005) |
| | Supply Chain | Lockamy and McCormack (2004) |
| | | Reyes and Giachetti |

| | | |
|---|---|---|
| | | (2010) |
| | Project Management | Ibbs and Kwak, (2000) |
| | | Crawford (2007) |
| | Assessment of Business Process Management | DeBruin and Rosemann (2005) |
| | Knowledge-based Decision Making | Kaner and Karni (2004) |
| | Risk Management Capability Maturity Model for Complex Product Systems Projects | Yeo and Ren (2009) |
| Capability Maturity Model Integration (CMMI) | Cloud Maturity Model | Duarte (2013) |
| | | Open Data Center Alliance (2013) |
| IT Capability Maturity Framework (IT-CMF) | Cloud Maturity Model | Conway and Curry (2012) |

## 5. The Cloud Maturity Model®

The Open Data Center Alliance is an IT consortium aiming at guiding organizations to move their IT operations to the cloud. This group is led by a steering committee of senior IT executives from different organizations[25]. They detail the roadmap taken by organizations to reach cloud maturity, through a cloud maturity model[26]. They identify the vital needs for a cloud maturity model in order to support the development of a cloud roadmap and strategy, comprehend the different areas comprising the cloud maturity, prioritize some areas over others depending on the organization's needs, and particularly achieve the anticipated advantages from adopting cloud solutions. This model parallels the Capability Maturity Model Integration by measuring cloud capabilities over six maturity levels.

### 5.1 Cloud Capabilities

The cloud maturity model describes maturity from the business and IT perspectives. These perspectives map business and IT capabilities in order to understand the adoption of cloud solutions from the business and IT point of views, respectively (ODCA, 2016).

[25] https://opendatacenteralliance.org/about-us/

[26] https://opendatacenteralliance.org/accelerating-adoption/cloud-maturity-model/

Business capabilities are classified into four business domains, including, business and strategy, organization and skills, governance, and projects, portfolios and services (ODCA, 2016). The business and strategy domain encompasses executive-level constructs allowing the implementation of cloud computing, such as motivation, expected benefits and costs, etc. The organization and skills domain represents the development of skills and competences adapted for cloud computing. In addition, the governance domain includes capabilities related to the governance structures and processes guiding adoption efforts. Finally, the last business domain is projects, portfolios and services encompassing the management of services portfolios while planning cloud services (ODCA, 2016).

On the other hand, IT capabilities are categorized into four domains; architecture, operations, infrastructure, and information (ODCA, 2016). The architecture domain defines the different guidelines for stakeholders aiming at a correct implementation of cloud solutions. The operations domain contains capabilities linked to the administration, operations and management characteristics of the cloud environment. The infrastructure domain provides technical capabilities for implementing cloud solutions (IaaS, PaaS and SaaS). Lastly, the information domain includes capabilities related to the information characteristics of cloud computing (ODCA, 2016).

## 5.2 Maturity Levels

The Cloud Maturity Model consists of five maturity levels; the initial or Ad Hoc level (CMM1), the repeatable or opportunistic level (CMM2), the defined or systematic level (CMM3), the measured level (CMM4), and the optimized level (CMM5) (not to confuse the acronym of the Cloud Maturity Model with the one of the Capability Maturity Model – also known under CMM). It is important to note that CMM0 exists and represents the legacy applications on dedicated infrastructure where no cloud approach has been adopted. Each maturity level represents a "*well-defined evolutionary plateau*" (Paulk et al., 1993, p.7) towards achieving improved processes. Progressing through the various levels of the model depends on the organization's ability to analyze and evaluate the capabilities in the different domains (ODCA, 2016).

CMM1 represents the initial level of adopting cloud solutions. In this level, organizations analyze their current environment to move potentially to a cloud environment (ODCA, 2016). While the organization still possesses its physical infrastructure, some virtualized systems exist already. However, they are operated under traditional IT processes and lack automation. Some cloud computing awareness is spread throughout the organization, while some teams are starting to adopt few cloud solutions. In addition, organizations feel safer at this stage to implement their private cloud, along with adopting some basic public SaaS solutions.

CMM2 is the repeatable or opportunistic level in a cloud maturity model. Processes are being defined, transformed and updated in order to deal with cloud solutions (ODCA, 2016). In this level, organizations fully embraced their private cloud while thinking of moving some applications to the cloud. For instance, cloud-aware applications are being part of the board's discussions. While an approach has been applied opportunistically, it has not been widely accepted yet.

CMM3 is the defined and systematic level of the cloud maturity model offered by the Open Data Center Alliance (ODCA, 2016). Here, the proposed approach in CMM2 has been finally reviewed and accepted by the various parties. The important part of this level is the introduction of governance and risk tools in the control layer. Organizations, hence, follow the corporate requirements and regulations. In addition, organizations observe an emergence of a private PaaS with a sophisticated implementation of SaaS solutions.

CMM4 refers to the measured level since the organizations' governance structures are deployed to measure cloud capabilities. At this stage, the organization is implementing cloud solutions according to the business departments' needs, whether on private, public or hybrid platforms (ODCA, 2016). In addition, tool layers integration, such as service desks, exist along with dynamic movement of systems and data. Organizations, hence, observe pervasiveness of PaaS solutions.

CMM5 is the final level of cloud adoption maturity, where organizations implement cloud solutions optimally, whether it is related to public, private, hybrid cloud and whether it is related to IaaS, PaaS or SaaS solutions (ODCA, 2016). Once organizations reach this level, all of its application and service adoptions are automated. In addition, the majority of the organization's landscape is constituted from cloud-aware applications.

## 5.3 Cloud Maturity Evaluation

The Open Data Center Alliance proposes to evaluate the maturity of the organization based on every domain included in their Cloud Maturity Model (ODCA, 2013). Therefore, the organization evaluates its level of maturity for each domain, in order to improve the domains that need development. Table 10 represents the evaluation of the organization's cloud maturity according to the business capabilities domains.

The cloud maturity model aims at assessing the organization's maturity and precisely recommending ways to improve. It allows organizations to compare the maturity of different domains, pushing them to improve the ones that need development. Maturity models provide numerous benefits for organizations. For instance, implementing a maturity model delivers real cost savings for organizations, where they can detect errors on earlier stages, increase cost predictability and reduce remediation costs. Through the self-assessment provided by a maturity model, organizations will be able to improve their processes, enhance their performance and differentiate from others and hence making them more competitive. Additionally, through competition, customers become more demanding, pushing organizations on supplying them with the correct product/service in the shortest time-to-market. If customers are unsatisfied, they can easily switch to one of the organization's competitors. Therefore, in order to keep their market shares, organizations are highly advised to adopt a maturity model in today's fast-growing market.

**Table 10: Business capabilities perspective of the Cloud Maturity Model**[27]

| | **CMM1** | **CMM2** | **CMM3** | **CMM4** | **CMM5** |
|---|---|---|---|---|---|
| **Business Strategy** | Ad Hoc use of cloud services<br><br>Business contact is missing | Departmental cloud strategies applied<br><br>Opportunistic leverage of cloud services | Enterprise cloud strategy exists<br><br>Funding decisions influenced by enterprise priorities | Cloud strategy is an integral part of business strategy<br><br>Generates significant Value | Federated, Interoperable, and Open Cloud:<br><br>Majority of landscape is cloud-aware applications<br><br>Automated provisioning according to business requirements |
| **Organization and Skills** | Purchase decisions are Ad Hoc<br><br>Low level of skills in | Islands of excellence of cloud skills<br><br>Departmental principles | Skills improve from operational to strategic<br><br>Guiding | Sound mix of strategic, business, and operational skills across | |

[27] Source: Open Data Center AllianceSM usage model: Cloud maturity model Rev. 2.5. Available at: https://opendatacenteralliance.org/docs/cloud_maturity_model_rev_2.5/

| | | | | | |
|---|---|---|---|---|---|
| | cloud services | exist to guide cloud decisions | principles are well known and adopted | the enterprise | and controls<br><br>Managed public, private, and hybrid SaaS, PaaS, IaaS provisioning and integration<br><br>Dynamic compliance and control |
| **Governance** | Disparate governance models and practices | Categorized business applications, data policies<br><br>Procurement processes and contracts for cloud | Cloud governance integrated within organizational governance practices | Risk and compliance management adds business value for cloud services<br><br>Metrics are used for decision making | |
| **Projects, Portfolios, and Services** | Cloud projects and changes occur with Ad Hoc controls and designs<br><br>Lifecycle of cloud projects do not intersect | Ad Hoc cloud service management<br><br>Basic infrastructure service catalog<br><br>Cloud projects are governed and managed inconsistently | Transition and transformation process for cloud<br><br>Mature project management competencies for cloud<br><br>Defined orchestration process for cloud | Planning functions for cloud services are mature<br><br>Build and run competencies for cloud projects and program of work exist | |

For example, when an organization evaluates its business strategy as "*an integral part of business strategy which generates significant value*" (column 5), then the organization will know that in the business strategy domain, their maturity is CMM4.

Table 11 represents the evaluation of the organization's cloud maturity according to the IT capabilities domains. For example, while the organization evaluates its information maturity, if it has "*Information-as-a-Service with complex PaaS and SaaS*" (column 4), then its maturity in the information domain is CMM3.

**Table 11: Technology capabilities perspective of the Cloud Maturity Model**[28]

<table>
<tr><th></th><th>CMM1</th><th>CMM2</th><th>CMM3</th><th>CMM4</th><th>CMM5</th></tr>
<tr><td>Operations, Administration and Governance</td><td>Scheduled Admin and Activities</td><td>Procurement Processes and Contracts for Cloud</td><td>Event-triggered Admin and Activities<br><br>Service Delivery Management including Cloud Interface</td><td>Automated Service Migration according to pre-defined cases (for example, costs)<br><br>Online risk and compliance management</td><td rowspan="4">Federated, Interoperable and Open Cloud:<br><br>Majority of landscape is cloud-aware applications<br><br>Automated provisioning according to business requirements and controls<br><br>Managed public, private, and hybrid SaaS, PaaS, IaaS provisioning and integration<br><br>Dynamic compliance and control</td></tr>
<tr><td>Information</td><td>Information Pools</td><td>Categorized Business applications, data policies</td><td>Information as a Service<br><br>Complex PaaS and SaaS</td><td>Integrated use cases for public, private, and hybrid</td></tr>
<tr><td>Architecture</td><td>Simple IaaS instances</td><td>Virtualized infrastructure applications<br><br>Complex IaaS<br><br>Simple federated IaaS<br><br>Simple IaaS</td><td>Islands of identity and access management<br><br>Simple SaaS<br><br>Standardized PaaS products<br><br>Orchestration tooling with API interfaces</td><td>Integrated security management<br><br>Hybrid SaaS<br><br>Hybrid PaaS<br><br>Transition and transformation tooling including cloud brokering</td></tr>
<tr><td>Infrastructure</td><td>Compute, storage, and network</td><td>Cloud-aware application development framework<br><br>Defined</td><td>Private SaaS Framework<br><br>Private PaaS Framework</td><td>Federated identity and access model<br><br>Architecture for federated</td></tr>
</table>

[28] Source: Open Data Center Alliance℠ usage model: Cloud maturity model Rev. 2.5. Available at: https://opendatacenteralliance.org/docs/cloud_maturity_model_rev_2.5/

| | | | |
|---|---|---|---|
| | orchestration process for cloud<br><br>Defined cloud service catalog | Transition and transformation process for cloud<br><br>Defined cloud architecture | cloud control systems |

In order to analyze the cloud maturity in the different domains, the Open Data Center Alliance simplified the task on organizations by proposing some assessment questions for each domain, as shown in Table 12.

**Table 12: Cloud Maturity Model assessment questions[29]**

| | **Assessment Question** | **CMM1** | **CMM2** | **CMM3** | **CMM4** | **CMM5** |
|---|---|---|---|---|---|---|
| **Business Strategy** | *Does a formal enterprise level strategy exist positioning the use of Cloud based services?* | No | Yes, but with ad-hoc adoption | Well communicated throughout the organization and signed off by all key stakeholders | Guides all new system deployments and technology renewals as "the rule". The coverage is measured by means of tracked KPI's | The cloud strategy enables the growth and optimization of business outcomes across the enterprise. The strategy is revised on a regular basis, according to a defined timeframe. |
| | *Is there a Cloud Adoption Framework ?* | The current application landscape has been analyzed for possible cloud migration | Classification framework for all Business Applications & Data, with all apps considered for cloud, classified | A cloud service adoption plan exists, with Milestones defined, planning, and budget | The use and success of the framework is managed by means of KPIs | New opportunities offered by cloud services are evaluated and included in the Cloud Adoption Framework on a regular basis |

[29] Source: Open Data Center Alliance[SM] usage model: Cloud maturity model Rev. 2.5. Available at: https://opendatacenteralliance.org/docs/cloud_maturity_model_rev_2.5/

| | | | | | | |
|---|---|---|---|---|---|---|
| | *Do Key Performance Indicators exist for cloud based services?* | Success of cloud services is evaluated by different users. There is no common definition of success. | KPIs are defined to measure the success of the cloud strategy | KPIs are agreed to measure the success of the cloud strategy | The KPIs are constantly measured, and the results are reviewed. | The definition of the KPIs are checked and reviewed regularly |
| **Organization and Skills** | *Has the organizational structure been updated to enable Cloud based Service delivery?* | No | Structure defined | Teams created. Cloud KPIs per team identified | Teams measured by KPIs. Active planning against gaps, and reviewed regularly | The organizational structure is able to bring tangible business benefits - and the operating model is an integral part of the culture, with defined KPIs |
| | *Is formal Cloud Training Planned?* | Incidental, Training in new topics is done by individual employees with personal commitment or interest | Training on new topics is discussed in teams with some organizational support. | A training and development plan exists and is implemented, defined per impacted business unit | The use and success of an enterprise training and development plan is ensured through product certifications, and other knowledge tests. | A training concept exists, which is constantly updated to align to the changes of the cloud strategy of the company. |
| | *Role of Internal IT?* | Continues handling internal IT and internal data center and outsourcing topics | A cloud capability exists, and IT participates in Cloud deployments | Clear positioning as a Cloud Provider or as a facilitator or broker, with updated skills and roles | Consults with Business on appropriate cloud platforms | Acts as a bridge between external providers, internal providers, and manages service definitions |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Governance** | *Does a formal Communication plan exist, positioning cloud and the impacts?* | Governance, risk and compliance requirements are available for those who look for them, for cloud services, documented in an enterprise repository | Limited positioning of cloud with respect to requirements and compliance are communicated to islands of adoption | A communication plan exists relating to cloud services, and detailed follow through activities with the impacted business units is ongoing, including a feedback mechanism, and regular progress reports, possibly via the enterprise communications vehicles. | Partners, clients and suppliers are addressed and cloud based implications clearly defined at service, commercial and business impact level | Co-ordinated roadmap updates and communications are broadcast through the full eco-system, with feedback loops in place |
| | *Is Risk Management updated for Cloud?* | Risks may be evaluated in project situations. No general risk definition | Risks are discussed (4-eyes principle) | Risks are known and documented. | A Risk management framework is defined and contextualized for cloud. Risks are constantly monitored. Risk mitigation plans are in place | A governance structure has been implemented to manage risks for the business. The risk mitigation plan is regularly updated. Computer Emergency Response Team (CERT) exists |
| | *Is there a formal Compliance framework for Cloud?* | Standard original compliance framework carries forward, without cloud awareness | A Compliance framework is defined and includes cloud appropriate | Compliance framework is updated to include cross border legislation, data protection in transit and at rest in cloud environments, and data privacy requirements dimensions | Categorization of requirements exists graded separately for Private, Hybrid, Public & Hosted cloud types. Monitoring and Management of compliance | The compliance framework is regularly updated to reflect changes in cloud services and usage. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | requirements is automated, sensitive per cloud category | |
| | *Do Cloud Contract templates exist?* | No, still using original templates | Leveraging contracts supplied by each cloud provider, with slightly different terms and conditions, and processes | Zero $ based framework contracts (agreements defining services and service level agreements, but with no volume commitments due to the nature of cloud services) are in place to enable service use, and all roles and responsibilities and remediation are clearly defined, including risk, compliance, and data related actions | Contracts with multiple suppliers are synchronized to common terms and processes, enabling the business to scale, migrate and adopt services transparently | All commercial terms are electronically integrated and linked to the service classes and qualities selected from the available catalogues, by the consumer |
| **Projects, Portfolio, and Services** | *Are Project Tools updated to support Cloud projects?* | Each project is defined by the assigned project manager, and built from scratch | Cloud based project templates are shared between project managers for re-use | Pre-defined elements are automatically populated into the project plan by the tool, and consistent feedback loops exist to update approved steps | Online project tool with integrated documentation is linked to selected cloud deployments and reporting systems. | Online project tool also integrates with and triggers / invokes workflows and processes for partnered services, as part of the Cloud Service landscape |

| | | | | | | |
|---|---|---|---|---|---|---|
| | *Do Project Skills exist for cloud projects?* | Few internal skills exist aligned to common organizational cloud designs | Cloud Infrastructure Skills exist and are available to support projects | Application developers are skilled in cloud use, aligned to the enterprise strategy, and available to support projects | Partnered skills from Cloud Providers are integrated into project teams, enabling internal resources to focus on corporate objectives | Online interfaces and controls are in place enabling skills to be sourced from wherever they may exist, for the specific requirement (i.e. skills requirements are placed on external tender to specialists) |
| **Architecture** | *Are Architecture Processes in existence for Cloud based services?* | Cloud based solution design is handled completely by lines of business | Templates for cloud platforms exist and some guidelines available for application layer | Full documentation of cloud architecture and existence of core cloud designs, up to application layer | Cloud design review document exist demonstrating compliance to or deviation from core cloud reference architectures. | Existence of operational metrics, used in conjunction with architecture governance scoring, producing a multi-dimensional score for cloud implementations. |
| **Operations** | *Are clear processes (e.g. ITIL) for service, risk and compliance management processes defined for cloud based services including Incident, Problem and Change Management and integrated with the consumer ecosystems?* | Individual human based service management is in place, responding to regular reports or events as they occur or are produced in arrears | Each cloud providers' own processes are used manually, with ad-hoc coupling to the consumer organisations' processes | Well defined processes exist and are consistent between consumer and all providers | Processes are supported by tooling to improve quality | All process by-passes or exceptions are automatically detected and real-time alerting occurs |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Infrastructure – for those who adopt IaaS** | *Is Management and Monitoring updated for Cloud based services?* | Ad Hoc reporting is based on providers' shared monitoring data | Standard interface exists receiving agreed monitoring and alerting data from selected providers | Automated deployment of and triggering of event monitoring and management is bound to each IaaS service, extending to SIEM | Data is managed according to defined lifecycles and policies | All data in landscape is managed according to a single set of policies and rules |
| **Infrastructure – for those who adopt PaaS** | *Is a PaaS framework available for the business to leverage for effective cloud application development?* | Ad-hoc development | Defined security providers, messaging facilities | Resilient design blueprints are available for common re-use of all key application elements | Auto-scaling, uses pre-built or scripted elements like web services, message bus's etc. | Interoperable design elements call external security providers and message busses, enabling cross-cloud application design and development |
| **Infrastructure – for those who adopt SaaS** | *Does an enterprise policy exist for the use of SaaS services and the resulting data sets?* | Individual human based service management is in place, responding to regular reports or events as they occur or are produced in arrears | Each cloud providers' own data protection offering is generally accepted | Well defined data policies exist and are consistent between consumer and all providers | Policies are supported by tooling and enterprise Confidential data is retained within the enterprise perimeter, while "generic data" is linked anonymously from the SaaS provider | All policy by-passes or exceptions are automatically detected and real-time alerting occurs |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Information** | *Are Security Skills updated to include Cloud?* | Skills are based on enterprise toolsets and do not address governance requirements | Training of staff includes cloud concepts and business objectives for cloud use, including governance aspects such as enterprise security | Consistent staff training occurs between all partners, suppliers and employees of the enterprise | Cloud Security training and certifications are required for all involved parties | Consistent Cloud security certification is aligned and required through the defined cloud eco-system of the corporation and its partners |

Through these assessment questions, organizations will be able to evaluate the cloud maturity in eight domains, and hence position themselves in the proposed levels. To do so, organizations assess themselves and allocate a cloud maturity level for each domain. Then, they take the average of the maturity of the eight domains and get their overall maturity. Through this self-assessment, organizations know which domain(s), or capabilities of a domain need to be improved.

To illustrate this, assuming an organization is self-assessing itself in the **organization and skills** domain. And assuming that while asking the assessment question "*is a formal cloud training planned?"* (CMM2 cell in Table 12), it gets a maturity level of CMM2; "*Training on new topics is discussed in teams with some organizational support*". Then, to be more mature in this domain (moving to CMM3, and therefore increasing its overall maturity), the organization knows that it needs to focus on "*implementing training and development plans for each impacted business unit*" (jumping to the next cell in Table 12 – CMM3). While the organization increases the maturity of its **organization and skills** domain, its overall maturity will automatically also increase. As noted by the Open Data Center Alliance (ODCA, 2013), organizations need around 18 months to move from one maturity level to the other. Therefore, optimizing maturity is a long process that is highly beneficial on the long term.

The Cloud Maturity Model proposed by the Open Data Center Alliance (ODCA, 2016) addresses a large amount of cloud computing aspects while covering the different angles. Therefore, this model is very suitable for our research work in order to first, assess the cloud maturity of our organizations and then, provide them with ways to improve it in the different mentioned domains.

# Research Design

The research design of this thesis is presented in this chapter. The author will start by exploring the existing methodological approaches present in the literature. Then, the possible philosophical epistemologies are elaborated, along with the various methods for data collection. While many disciplines use different approaches, the aim of this chapter is to argue of the most suitable approach in order to answer the proposed research question. Furthermore, it is very important to understand the philosophy behind the conducted research. Therefore, based on the research question and on the literature review presented in the previous chapter, the author argues of the most appropriate methodological approach and philosophical epistemology adopted in this research work. In addition, the methods used through two phases of data collection and data analysis are explored in this chapter.

# I. Methodological Approach

Our extensive literature review on IS studies, and more specifically on IT and cloud governance, shows limited existing research on the way large organizations can govern their cloud solutions. Hence, an exploratory research methodology appears to be useful in order to address a subject that is not very well investigated and understood: how large organizations should effectively govern their cloud solutions while minimizing risks, increasing benefits, and optimizing their cloud adoption.

This section aims at describing the most suitable research design for our research. To avoid any confusion, it is important to start this chapter by clearly differentiating between the methodology, the methods, and the design. Cresswell (2013, p. 4) defines the methodology as "*the philosophical and fundamental assumptions of research that relate to the entire process of research*", the methods as "*the techniques of data collection and analysis*" and the design as "*the plan of action that links the philosophical assumptions to the specific chosen methods*". Greener (2008) also agrees on the importance of differentiating between methodology ("*researcher's attitude and understanding of research, and the strategy chosen to answer the research question*", p. 10), and methods ("*specific activities designed to generate data*", p. 10). Therefore, based on the definitions proposed by Cresswell (2013) along with Greener (2008), the aim of the methodology section is to describe the chosen methodology in order for the thesis to be replicated. In addition, this section aims at exploring the motivation behind the methodological choices deployed in order to focus on the research question. On the other hand, the purpose of the methodology section is not only to evoke the validity or our choice, but the limitations as well.

According to Holden and Lynch (2004), it is very important for authors to understand the philosophy behind their research. This knowledge will enrich their research skills as well as enhance their confidence, guiding them to the most appropriate methodological choice. Several research disciplines use different research approaches. Choosing an appropriate research approach is challenging to every researcher in any field, especially in the Information Systems field, being multi-disciplinary. Therefore, choosing an appropriate research approach for our subject constituted a major process, where we based our choice on the most appropriate angle to address our research questions. For instance, scanning the methodology literature resulted in the statement that researchers are supposed to base their decisions on the nature of their work, where no one approach is better than the other (Malterud, 2001).

Three types of research approaches exist: qualitative, quantitative, a mixture of both (Cresswell, 2013). While quantitative research focuses primarily on numerical data and statistical interpretations, qualitative research deals with large amount of textual data and interpretations that are tied with human experiences, senses and subjectivity. The positions of researchers regarding mixing these two approaches vary considerably. For some researchers, mixing these two approaches can be complementary (Bryman, 1988). Combining quantitative and qualitative approaches can help the researcher to better understand complex phenomenon such as the "*messy world of people and organizations*" (Greener, 2008). However, some orthodox researchers have proclaimed that mixing these two approaches is neither appropriate nor consistent (Freshwater and Cahill, 2013).

Hence, researchers have different opinions regarding both qualitative and quantitative approaches. Although some value the qualitative approach as it provides a deeper understanding of a situation through dealing with data closer to reality than numbers, others prefer the robustness of quantitative approaches that are considered as more 'scientific' and 'objective' (Hughes, 1997). Furthermore, researchers often consider that qualitative research forms address questions beginning with why, how, and what, whereas quantitative research forms address ones beginning with how many or how much.

Fitzgerald and Howcroft (1998) classified different characteristics to both approaches, resumed in the following Table 13.

**Table 13: Research approaches characteristics – Based on Fitzgerald and Howcroft (1998)**

| Research Approach | Characteristics |
|---|---|
| Qualitative | **Definition**<br>Determining what things exist rather than how many there are. Thick description. Less structured and more respective to needs and nature of research situations. |
| | **Interpretivism**<br>No universal truth. Understand and interpret from researcher's own frame of reference. Uncommitted neutrality. Realism of context important. |
| | **Exploratory**<br>Concerned with discovering patterns in research data and to explain/understand them. Lays basic descriptive foundation. May lead to generation of hypothesis |

| | |
|---|---|
| | **Induction**<br>Specific instances used to arrive at overall generalizations. Criticized by many philosophers of science but plays an important role in theory/ hypothesis conception. |
| | **Field**<br>Emphasis on realism of context in natural situation, but precision in control of variables and behavior measurement cannot be achieved. |
| | **Idiographic**<br>Individual-centered perspective which uses naturalistic contexts & qualitative methods to recognize unique experience of the subject |
| Quantitative | **Definition**<br>Use of mathematical and statistical techniques to identify facts and causal relationships. Samples can be larger and representative. Results can be generalized to larger populations within known limits of error. |
| | **Positivism**<br>Belief that the world conforms to fixed laws of causation. Complexity can be tackled by reductionism. Emphasis on objectivity, measurement and repeatability. |
| | **Confirmatory**<br>Concerned with hypothesis testing and theory verification. Tends to follow positivist, quantitative modes of research. |
| | **Deduction**<br>Uses general results to ascribe properties to specific instances. Associated with theory verification and hypothesis testing. |
| | **Laboratory**<br>Precise measurement and control of variables, but as expense of naturalness of situation, since real-world intensity and variation may not be achievable. |
| | **Nomothetic**<br>Group-centered perspective using controlled environments & quantitative methods to establish general laws |

Based on this classification, researchers assume that qualitative approaches draw on interpretivism whereas quantitative approaches draw on positivism. While the interpretative paradigm aims at understanding the reality from people's perspectives and interpretations, the positivism is associated with testing hypothesis and correlating two or more variables. Similarly, quantitative approaches are generally associated with the use of questionnaires to collect data, whereas qualitative approaches are associated with observations and the use of interviews to collect data. However, this distinction between quantitative and qualitative approaches has been questioned and a subject to many debates. Without taking part of this debate, we agree that the choice of any research approach should be linked to the research objectives. According to Holden and Lynch (2004), researchers should not lead their research methodology. Instead, they should select their methodology based on the nature of the studied phenomenon. Whenever researchers are working with a new phenomenon demanding a deep understanding, a clear explanation and a detailed interpretation, they are advised to use the qualitative approach in order to explore such phenomena through new perceptions, perspectives and experiences achieved by participants (Skinner et al., 2000 and Broom et al., 2009).

Researchers studying and exploring the organizational processes, goals, success or failure of a new phenomenon are advised by to use a qualitative approach (Skinner et al., 2000; Broom et al., 2009). Considering the nature of our research objective, we draw this thesis on a qualitative research form.

However, the qualitative research approach presents strengths as well as limitations. On the positive side, it first allows phenomena to be studied in their natural setting (Benbasat et al., 1987; Maykut and Morehouse, 1994) and context-specific setting (Stake, 1995; Myers, 1997; Silverman, 2000). In addition, researchers can generate theories from practice under the qualitative umbrella (Benbasat et al., 1987; Myers, 1997), as well as investigate meanings given by the participants (Silverman, 2000). As researchers gain in-depth understanding of the phenomenon nature and complexity (Benbasat et al., 1987; Maykut and Morehouse, 1994; Silverman, 2000), barriers between them and the participants are lowered in a qualitative approach (Stake, 1995). On the other side, qualitative approach possesses negative characteristics. When dealing with qualitative empirical material, the researcher is analyzing a smaller sample size than other approaches, which reduces generalizability and deductibility (Cornford and Smithson, 2006; Lee, 1991; Maykut and Morehouse, 1994; Silverman, 2000). In addition, as the collection of data is unbounded (Lee, 1991), it demands a large amount of time followed by transcribing and analyzing it (Miles and Huberman, 1994; Lee, 1991). Moreover, the textual material is prone to be lost through multiple interpretations (Cornford and Smithson, 2006; Silverman, 2000), as well as summarization (Lee, 1991; Miles and Huberman, 1994), which might reduce its accuracy.

Cloud computing has been a subject of interest for a large part of organizations worldwide, where its adoption has been increasing. Even though quantitative tools, such as questionnaires, are a convenient method to check the governance of cloud solutions for French organizations, qualitative methods, such as conducting interviews with appropriate employees, would reveal more in-depth details overlooked by questionnaires. Therefore, we decided to adopt a qualitative approach, which is more relevant in our case for several reasons: first, we are interested with the perceptions, opinions and views regarding organizations' experiences with cloud solutions. Hence, qualitative data is useful when it comes to defining views, beliefs, feelings and attitudes as well as reducing barriers between the researcher and participants (Stake, 1995). In addition, it is helpful to understand meanings and interpretations given the cloud computing phenomenon in French organizations. Finally, a qualitative approach is also necessary in order to build inductively frameworks regarding the adoption of cloud services, and understand the ways French organizations govern and deal with such services. Qualitative data will shed the light on individuals' experiences, attitudes and motivations, which will help in better understanding this relatively-new phenomenon, characterized by high levels of uncertainty.

In addition to the impact of the nature of the studied phenomenon, the philosophical assumptions related to the underlying epistemology will also guide the researcher in their research design. The following section will explain the different philosophical epistemologies that have been deployed in the literature and will highlight the underlying philosophical assumptions of this research work.

## II. Philosophical Epistemology

Every research study is based on some philosophical assumptions about what constitutes 'valid' research and how knowledge is obtained in a given study (Hirschheim, 1992). The selection of a paradigm will therefore guide the researcher in conducting his work. According to Kuhn (1974), the concept of paradigm refers to "*a research culture with a set of beliefs, values, and assumptions that a community of researchers has in common regarding the nature and conduct of research*" (p. 2). This concept has been also defined by Guba and Lincoln (1994) as a representation of a worldview "*that defines, for its holder, the nature of the 'world', the individual's place in it, and the range of possible relationships to that world and its parts, as, for example, cosmologies and theologies do*" (p. 107).

Different paradigms exist. While Guba and Lincoln (1994) suggest four underlying 'paradigms' for qualitative research (positivism, post-positivism, critical theory, and constructivism), Orlikowski and Baroudi (1991) who agree with Chua (1986), suggest three 'paradigms' that are mostly deployed in qualitative research: positivism, interpretivism, and critical (Figure 16). Before justifying the choice of the philosophical paradigm that guides our research, we start by defining the existing ones. According to Myers (1997), the positivism paradigm assumes that "*the reality is objectively given and can be described by measurable properties which are independent of the observer/researcher and his or her instruments*" (p. 5). Researchers take a positivist stand when they aim at testing a theory, dealing with quantifiable measures of variables, studying a phenomenon from a sample population. Positivism is largely used among researchers. On the other hand, the interpretivism paradigm assumes that "*reality (given or socially constructed) is only through social constructions such as language, consciousness and shared meanings*" (p. 5). Walsham (1995) also states that in the Information Systems field, interpretive studies "*aim at producing an understanding of the context of the IS, and the process whereby the information system influences and is influenced by the context*" (p. 4-5). The interpretivism paradigm accentuates the need to contextualize the analysis (Reeves and Hedberg, 2003). Finally, the critical paradigm is defined as researchers assuming "*that social reality is historically constituted and that it is produced and reproduced by people*" (Myers, 1997, p. 5). Researchers hence use critique to gain knowledge. For instance, along with an emancipatory perception, critical researchers focus on conflicts, oppositions and contradictions in today's society.

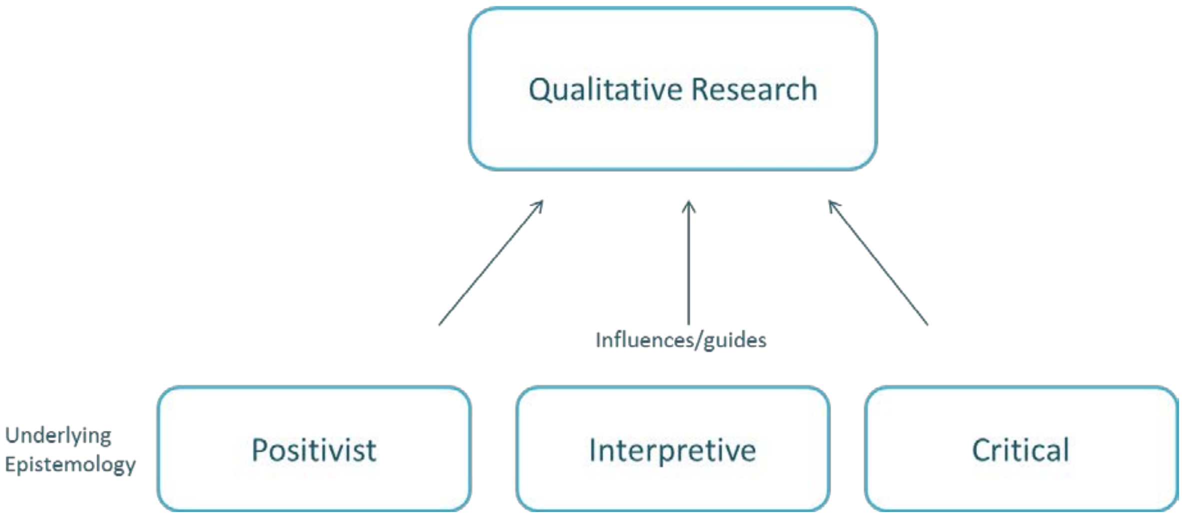


**Figure 16: Underlying philosophical assumptions – Based on Myers (1997)**

However, Guba and Lincoln (1994) proposed a fourth paradigm denoted "post-positivism". They defined post-positivism as "*the efforts of the last decades to respond in a limited way to the most problematic criticisms of positivism*" (p. 109). For instance, when adopting a post-positivism philosophical epistemology, researchers are first, critical about the findings, stating that they are probably true (unlike in positivism where findings are true), and second, they perceive reality as ‘real’ but only probabilistically apprehensible. Furthermore, according to Guba and Lincoln (1994), the four philosophical approaches are characterized with three dimensions: ontology, epistemology, and methodology. The ontology represents the nature of things, the epistemology constitutes the way researchers know about the nature of things along with their reality, and finally the methodology is the methods and techniques researchers deploy to find out about these things. These characteristics are represented in the following Table 14, based on Guba and Lincoln (1994).

**Table 14: Basic beliefs of alternative inquiry paradigms (source: Guba and Lincoln, 1994)**

| | **Positivism** | **Post-positivism** | **Constructivism/ Interpretivism** | **Critical** |
|---|---|---|---|---|
| **Ontology** | Naïve realism – “real” reality but apprehendable | Critical realism – “real” reality but only imperfectly and probabilistically apprehendable | Historical realism – virtual, reality shaped by social, political, cultural, economic, ethnic, and gender values; crystallized over time | Relativism – local and specific constructed realities |
| **Epistemology** | Dualistic/objectivist; finding true | Modified dualist/objectivist; critical tradition/community; findings probably true | Transactional/ subjectivist; value-mediated findings | Transactional/ subjectivist; created findings |
| **Methodology** | Experimental/ manipulative; verification of hypotheses; chiefly quantitative methods | Modified experimental/ manipulative; critical multiplism; falsification of hypotheses; may include qualitative methods | Dialog/dialectical | Hermeneutical/ dialectical |

In the IS field, along with Orlikowski’s research work (1993), the adoption of the interpretivism research approach has been increasing. However, the assumption of linking interpretivism with the qualitative approach and positivism with the qualitative approach is “*crude*” as noted by Mingers (2003, p. 236). He argues that the nature of the data used (whether empirical material or numbers and quantities) should not influence and be influenced by the philosophical view of the researcher. For example, Yin (2003) bases himself on a qualitative research approach with a positivist philosophy, whereas Glaser and Strauss (1967) base themselves on a mixture of qualitative and quantitative approaches with an interpretivist philosophy. Myers (1997) also clearly supports the argument that qualitative research is not a synonym for interpretivism.

As previously mentioned, cloud computing is an emerging new technology that has been present in the literature for a couple of decades. The adoption of cloud services is proven to be increasing. This is linked to the reality created socially, politically, culturally, and even economically. In addition, one can affirm that knowledge regarding the reality of cloud technologies is gained through social constructions. Plus, while knowledge related to such technologies is hard to be considered 'real' reality due to the lack of objectivity, having a subjective eye to deal with cloud computing from different angles is primordial. Consequently, to answer our research question, we decided that the most appropriate philosophical epistemology would be through interpretivism.

Now that the qualitative research approach is agreed on, and the philosophical epistemology is set, choosing the appropriate methods to answer our research questions is the next step. The following section will introduce the types of methods used in a qualitative approach where the research question is addressed from an interpretivist perspective.

## III. Methods for Data Collection

### 1. Observations

Observations are a very important method used in qualitative research. We are aware that fieldwork qualitative observations possess several advantages, such as, a better understanding and capture of the employees' interaction context, a lower dependence on prior documentation through being on site, and noticing things neglected by employees due to their routines (Patton, 2002). Nonetheless, in the words of Patton (2002) "*observations involve an enormous energy and concentration*" (p. 261). Therefore, observations would be inappropriate due to the nature and objective of our research work, where focusing on a single study in order to observe a phenomenon is not enough to answer our research questions. For instance, our main objective is to explore the way organizations govern their IT when adopting cloud solutions, which is a subject not well investigated. While observing different contexts would definitely provide us with rich information, conducting interviews in different contexts is more convenient due to the time limitation.

## 2. Interviews

According to Benbasat et al. (1987) interviews are the type of methods mostly used by researchers using a qualitative approach, due to the in-depth and detailed data collection. Fielding and Lee (1991) agree that interviews are one of the most important sources in qualitative research. There are three forms of interviews: structured interviews, semi-structured interviews, or unstructured interviews (Bryman and Bell, 2015). Structured interviews consist of well-prepared, specific, standardized and planned questions in advance asked throughout the whole interview. Semi-structured interviews consist of pre-determined questions asked in an open-end format and a sequence that is not fully planned in advance. Unstructured interviews comprise unprepared and unspecific questions that will be developed throughout the interview, based on the participant’s statement.

No one format is better than the other, since it all depends on the objectives and the requirements sought by the researchers at the end of the interview. For instance, while participants in a structured interview cannot divert from the prepared questions, they get to generate new ideas and explore new themes in a semi-structure interview. In addition, participants of a structured interview have the same set of answer options during the process, whereas participants of a semi-structured interview are more flexible. Semi-structured interviews are appropriate for exploratory research as they allow the researcher to gather insights and understanding instead of simply specific detailed answers (Newton, 2010). However, semi-structured interviews are time-consuming as the participants can go off track, which is disadvantageous when the researcher is limited by their time.

Interviews are a method used by researcher in order to support their methodology approach along with the chosen philosophical epistemology. This method of collecting empirical material is done through asking questions to the selected participants in order to discover the way they think and feel regarding the phenomenon in question (Collis and Hussey, 2013). In addition, interviewing participants is an important method as it allows researchers to collect more information and get more details about their studied subject. In addition, it allows them to get more information about the participants’ perceptions related to the studied issues. The aim of interviews is defined by Opendakker (2006, p. 1) as “*descriptions of the life-world of* *the interviewee with respect to interpretation of the meaning of the described phenomena*". He affirms that although face-to-face interviews are mostly used by researchers, interviews made through the phone or by the Internet are becoming popular. Nevertheless, according to Leedy and Ormrod (2001), face-to-face interviews are more effective and allow clearer answers, where the researcher can pay more attention to the participants' gestures and emotions. Moreover, such interviews allow researchers to inquire detailed and complicated questions while clarifying ambiguities and controlling the progress of the interview (Bowling and Ebrahim, 2005).

## 3. Documentation

Furthermore, documentation is another method that is used when researchers adopt a qualitative approach. Secondary data possess a large number of benefits for researchers. While Ghauri and Grønhaug (2005) state that secondary data is very advantageous as it saves time and money, Yin (2003) focuses on the fact that such data can be reviewed repeatedly, and hence interpreted more accurately. In addition, relying on secondary data represents a way to use data that cannot be collected by the researcher alone. Any of the following documentation is appropriate to analyze: website information, administrative documents, governmental whitepapers, organizational records, letters, agenda, newspaper, etc.

The following Table 15 cites the strengths along with the weaknesses of the interview and documentation methods and is partially retrieved from Yin (2013).

**Table 15: Strengths and weaknesses of types of methods – Based on Yin (2013)**

| | **Interviews** | **Documentation** |
|---|---|---|
| **Strengths** | Questions targeted, focus directly on research subjects<br>Detailed and insightful information | Documents can be reviewed repeatedly<br>Documents contain accurate and exact information, including names, references and organizational details<br>Document encompasses a broad span of time, events, settings |
| **Weaknesses** | Poor construction of questions<br>Biased Response | Documents cannot always be retrievable<br>Documents can be incomplete, |

| | | |
|---|---|---|
| | Some possible inaccuracies<br>Reflexivity where the interviewee gives what the interviewer wants to hear | leading to biased information<br>Hard to access documents |

As previously mentioned, due to the nature of our research work – an exploratory study – and time limitation, our empirical material encompasses two types of methods, which we will elaborate in the following sections.

## 4. Methods Used

The aim of our research work is to answer the following research question: *Does the deployment of cloud services require a specific governance model?* In order to answer this question and after contemplating on the most appropriate research methodology and epistemology, we decided to choose interviews and documentations as methods for collecting data. Table 16 describes the different methods adopted in our research work.

**Table 16: Methods adopted in our research work**

| | | | | |
|---|---|---|---|---|
| **Interviews** | Phase I | Contacting Potential Participants | Period | August 2015 to January 2016 |
| | | Data Collection | Type | Semi- Structured |
| | | | Period | November 2015 to April 2016 |
| | | Data Analysis | Method | Nvivo Coding |
| | | | Period | August 2016 to October 2016 |
| | Phase II | Contacting Participants | Period | November 2016 to January 2016 |
| | | Data Collection | Type | Structured |
| | | | Period | January 2017 to March 2017 |
| | | Data Analysis | Method | Analyzing Average Maturity |
| | | | Period | April 2017 to May 2017 |
| **Documentation** | | Data Collection | Type | Informative Emails; Reference material |

| | | | |
|---|---|---|---|
| | | | and other websites; Documents stating some organizational processes, missions, etc. |
| | | Period | During and Post Phase I of Interviews |

## 4.1 Phase I – First Round of Interviews

### 4.1.1 Data Collection

Regarding the conducted interviews, Myers and Newman (2007) noted that researchers in the Information Systems field mostly adopt semi-structured interviews. Therefore, in order to explore the way large French organizations govern their IT when adopting cloud solutions, and the link between their IT governance and their cloud computing maturity, our first round of interviews was in a semi-structured format with business and IT employees. The organizations participating in this study stem from a broad range of private and public sectors. The interviews took place between November 2015 and April 2016 and lasted between 35 and 88 minutes (59.5 minutes on average). Our focus on large organizations was motivated by prior research that has provided evidence for cloud computing implementations being more challenging for larger organizations (Winkler et al., 2014; Venters and Whitley, 2012). Moreover, large organizations present more complex contexts where cloud adoption is more interesting to explore. Our participants have advanced qualifications in business and IT subjects, where all of them are graduates from a prestigious engineering school or a business school, with at least a master's level. In this first round, we started by approaching a vast number of large French organizations (total of 143) that adopt cloud services. We identified these organizations through a professional association – the school alumni website – and through the contacts of other participants. However, after the first round of emails, we ended up with a total of 35 organizations, willing to go through the whole interview process. *De facto*, Mason (2010) studied 560 PhD theses to conclude that the average size of interviews for a qualitative approach is 31. Therefore, we were satisfied with interviewing 35 organizations. The following Table 17 represents a description of the participants' characteristics, including their fields (business or IT), their roles (CEOs, CIOs, IT managers, etc.), their industries (insurance, transport, utilities, etc.), their sectors (public or private), their locus of decisions (decentralized or centralized IT governance), the cloud service models adopted (IaaS, PaaS, and/or SaaS), along with the interview length.

**Table 17: Description of interview data**

| **Ref.** | **Field** | **Role** | **Industry** | **Sector** | **Locus of decisions** | **Services** | **Interview Length (min)** |
|---|---|---|---|---|---|---|---|
| B.1 | Business | CEO | Research Center | Public | Decentralized | IaaS, SaaS | 49 |
| IT.1 | IT | CIO | Retirement Insurance | Private | Centralized | PaaS, SaaS | 55 |
| IT.2 | IT | CIO | Transport | Private | Decentralized | IaaS, SaaS | 67 |
| IT.3 | IT | Senior IT project Manager | Transport | Private | Centralized | IaaS, PaaS, SaaS | 71 |
| IT.4 | IT | CIO | Retail | Private | Centralized | IaaS, SaaS | 61 |
| IT.5 | IT | Senior IT project Manager | Insurance | Private | Decentralized | IaaS, SaaS | 62 |
| IT.6 | IT | CIO | Bank | Private | Centralized | IaaS, PaaS, SaaS | 63 |
| IT.7 | IT | CIO | Media and Entertainment | Private | Decentralized | IaaS, SaaS | 81 |
| IT.8 | IT | Cloud Computing project Manager | Insurance | Private | Decentralized | IaaS, SaaS | 58 |
| IT.9 | IT | CIO | Family Insurance | Public | Centralized | IaaS, SaaS | 58 |
| IT.10 | IT | CIO | Retirement Insurance | Public | Centralized | IaaS, PaaS, SaaS | 62 |
| IT.11 | IT | CIO | Utilities | Private | Decentralized | IaaS, SaaS | 88 |
| IT.12 | IT | CIO | Utilities | Private | Decentralized | IaaS, SaaS | 53 |
| IT.13 | IT | CIO | Manufacturing | Private | Centralized | IaaS, PaaS, SaaS | 62 |
| B.2 | Business | CEO | Manufacturing | Private | Decentralized | SaaS | 42 |
| B.3 | Business | CEO | Social | Public | Decentralized | IaaS, SaaS | 35 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | Declarations | | | | |
| IT.14 | IT | Senior IT project Manager | Utilities | Private | Decentralized | IaaS, SaaS | 85 |
| B.4 | Business | Senior project Manager | Healthcare | Private | Centralized | IaaS, SaaS | 52 |
| B.5 | Business | CEO | Manufacturing | Private | Decentralized | IaaS, SaaS | 48 |
| IT.15 | IT | CIO | Postal Services | Private | Decentralized | IaaS, SaaS | 64 |
| B.6 | Business | Cloud Computing Project Manager | Utilities | Private | Decentralized | IaaS, SaaS | 68 |
| B.7 | Business | CEO | Manufacturing | Private | Decentralized | IaaS, SaaS | 64 |
| B.8 | Business | CEO | Media and Entertainment | Private | Centralized | IaaS, PaaS, SaaS | 70 |
| IT.16 | IT | CIO | Telecommunications | Private | Decentralized | IaaS, SaaS | 75 |
| IT.17 | IT | CIO | Power Transmission | Private | Decentralized | IaaS, SaaS | 42 |
| IT.18 | IT | CIO | Manufacturing | Private | Decentralized | IaaS, SaaS | 45 |
| IT.19 | IT | Interministerial Assistant Director of State IT (CIO) | First Minister Services | Public | Centralized | IaaS, SaaS | 47 |
| IT.20 | IT | CIO | Public Action | Public | Centralized | IaaS, SaaS | 48 |
| IT.21 | IT | CIO | Financial Services | Public | Centralized | IaaS, SaaS | 65 |
| B.9 | Business | CEO | Retail | Private | Decentralized | IaaS, SaaS | 57 |
| IT.22 | IT | Senior IT project Manager | Bank | Private | Centralized | IaaS, SaaS | 78 |
| B.10 | Business | CEO | Manufacturing | Private | Decentralized | IaaS, SaaS | 49 |
| IT.23 | IT | CIO | Higher Education | Public | Decentralized | IaaS, PaaS, SaaS | 59 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| B.11 | Business | CEO | Manufacturing | Private | Centralized | IaaS, SaaS | 45 |
| IT.24 | IT | Senior IT project Manager | High Tech | Private | Decentralized | IaaS, SaaS | 54 |

Figure 17, Figure 18, and Figure 19 represent the participants' sectors, roles, and fields proportions, respectively. In addition, Figure 20 represents the cloud services proportions among the 35 organizations, where Figure 21 represents the combinations of different services among these organizations.

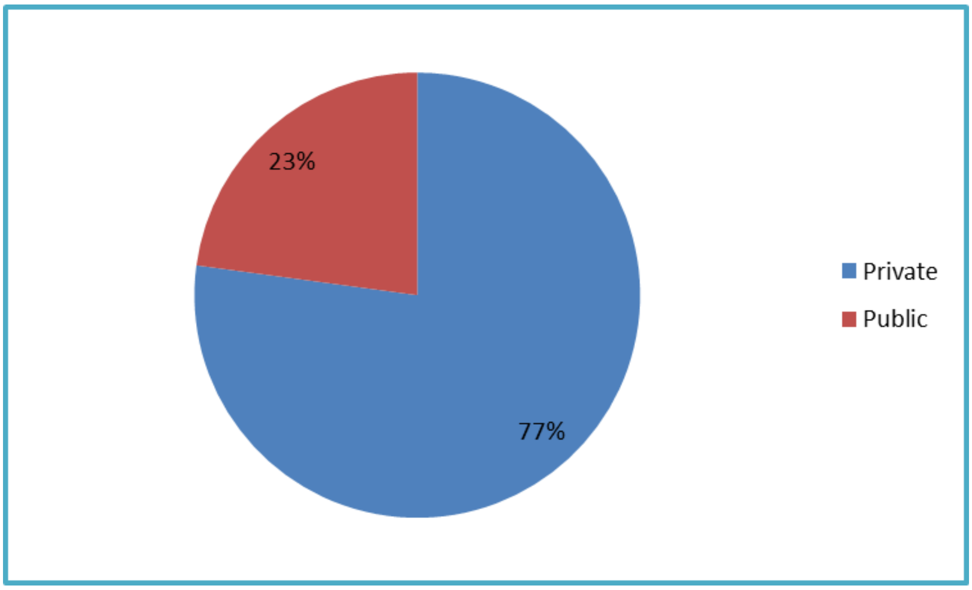


**Figure 17: Participants' sectors proportions**

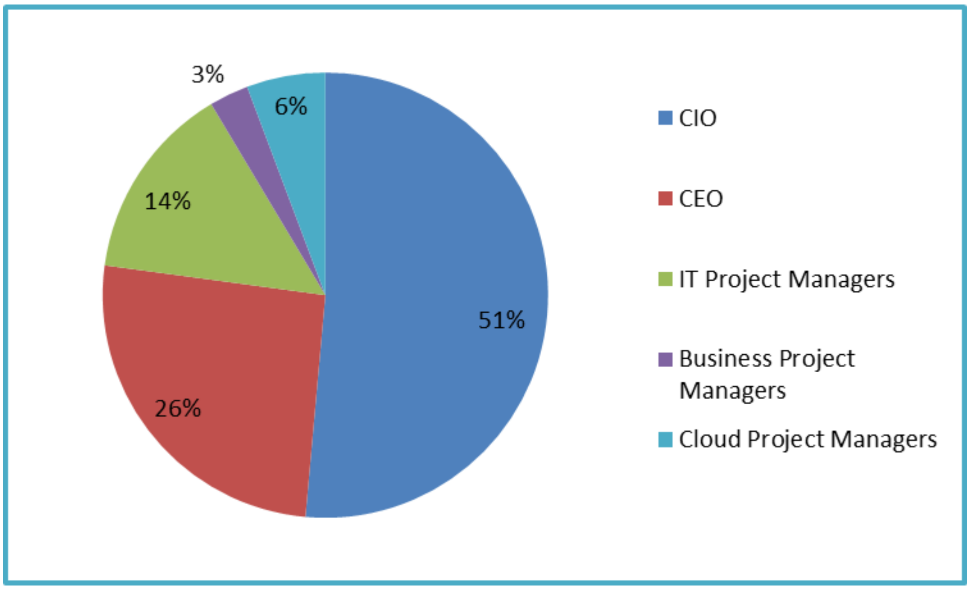


**Figure 18: Participants' roles proportions**

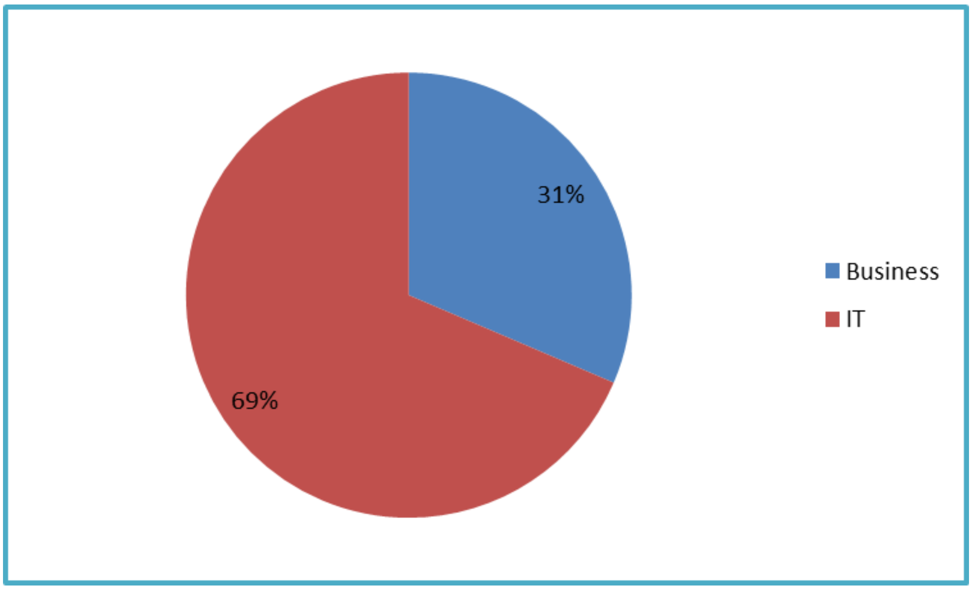


**Figure 19: Participants' fields proportions**

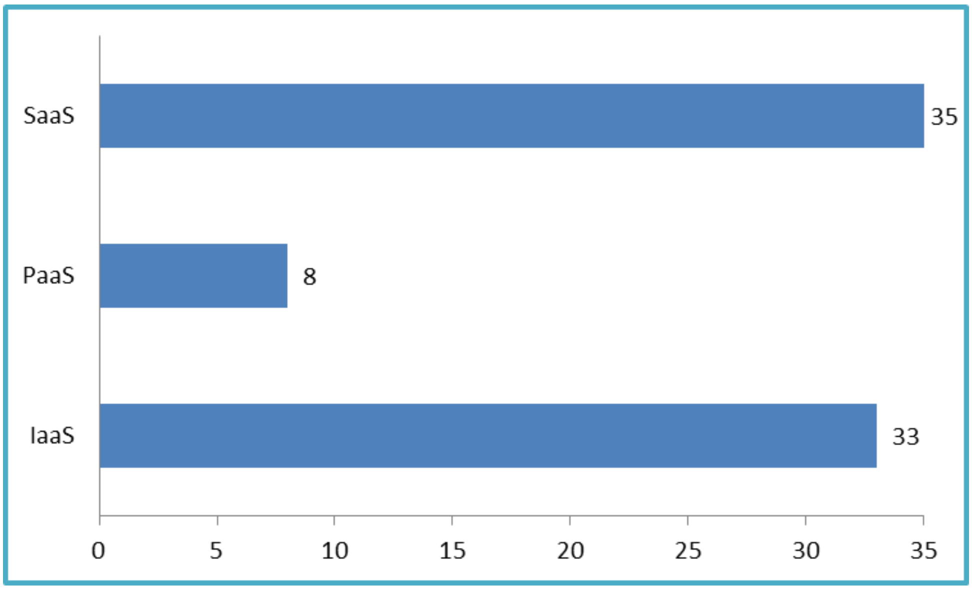


**Figure 20: Cloud services proportions**

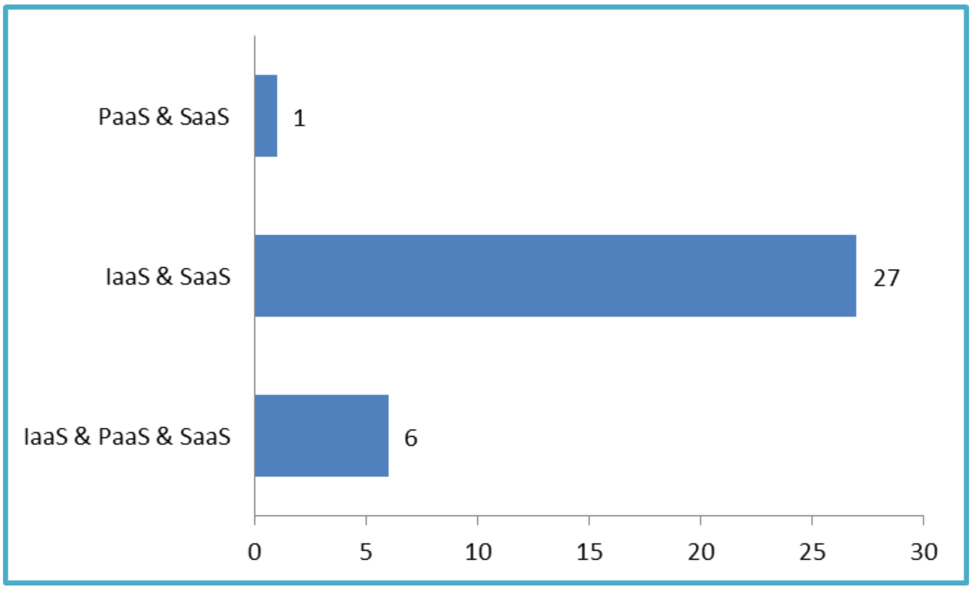


**Figure 21: Cloud services combinations proportions**

Our semi-structured interview guide discussed in detail the adoption of cloud computing by organizations. It can be found in the Appendix I. The major questions of the guide covered the interviewees' different opinions regarding cloud computing (benefits and risks), the reasons behind increasing or decreasing cloud usage, the way their organizations govern IT with new mechanisms (structures, processes, and relational) adapted to cloud computing, and finally the way cloud solutions have affected the organization.

Most interviews were recorded by highly-sensitive audio recording systems, with the consent of the participants (nonetheless, due to some strict confidentiality issues, 4 participants did not wish to be recorded – B.1, B.2, B.3, and B.5. Thus, quotes from these participants were only taken from the written notes during the interviews). In addition to recording, notes were taken during the interviews, mentioning important points. All of the interviews were then fully transcribed and analyzed using the software Nvivo v11, which will be elaborated in the following section.

We based our interviews on almost all the guidelines proposed by Myers and Newman (2007), where: we were situated as actors (guideline 1), we minimized social dissonance (guideline 2), we considered everyone as an interpreter (guideline 4), we used mirroring in our interviews questions and answers (guideline 5) while being flexible (guideline 6), and finally we provided them a confidentiality of disclosure (guideline 7). These points will be now elaborated. However, it is important to note that due to the difficulties we faced to find participants willing to discuss confidential issues regarding their adoption of cloud services, we were not able to interview more than one employee per organization during this round (guideline 3). Therefore, the third guideline proposed by Myers and Newman (2007) was not met during our interviews.

First of all, after more than a year of research in the IS field, regarding the management of cloud computing, we acquired a solid basis of knowledge in the field. Having chosen a wide subject such as the management of cloud computing, our research addressed it from several angles at first. Then, we were able to concise the different angles into the current one; governing cloud computing in French organizations. We conducted these interviews with a clear objective; building a relationship with the interviewees instead of interviewing them as neutral researchers. This objective was important for us in order to create a circle of trust and hence, to facilitate our discussions while minimizing barriers.

In addition, according to Klein and Myers (1999), when researchers implement an interpretive approach, they assume that the knowledge of reality is only gained through social constructions, whether through the use of language, tools, documents, technologies, or the shared meaning of actors and structure. The interpretive approach is not adopted to predefine dependent and independent variables or their causal relationships. In addition, in the words of Nicholson and Sahay (2004) "*the interpretive approach aims at understanding the complexity of human sense making processes, and the processes by which inter-subjectivity is obtained as the situation is constantly changing*" (p. 338). This leads to the conclusion that when researchers adopt the interpretive approach, they should assume that everyone is an interpreter. We took this conclusion into consideration when conducting our interviews. Finally, during the emails exchange with our potential interviewees, we introduced ourselves by explaining our identities and the purpose behind leading these interviews. The interviews were conducted at the organizations' premises. In addition, we started with reminding the interviewees with our purpose, and assuring them with a total confidentiality of disclosure, where even if the interviews were going to be recorded, their visions and opinions will not be personally attributed in any subsequent document. Once the interviewees agreed on that confidentiality, we started recording them for an average of an hour. However, as previously mentioned, 4 interviewees wished not to be recorded for strict confidentiality issues. We, surely, respected their choices. All of the interviews were semi-structured, where we began with inquiring about the organization's history and its progression towards cloud computing. We had a minimal script with key questions regarding their adoption and governance of cloud solutions, which evolved into more in-depth subjects. Throughout the interviews, we used the mirroring method where our interviewees were able to express freely their opinions on subjects they considered more important than others.

After laying out the data collection phase, the following section will describe the data analysis phase of the first round of interviews.

### 4.1.2 Data Analysis

There are several qualitative data analysis methods (Gibbs, 2002). *De facto*, data analysis refers to methods aiming at synthesizing empirical material, including interviews, documents, pictures, newspapers, etc. Due to the textual and narrative form of "data" in a qualitative approach, the analysis phase is not an easy task. In addition to its non-mathematical nature complexity, analyzing textual data demands a lot of time, first, to analyze the meanings of people's words, then to identify clusters of themes and patterns, and finally, to represent them as categories (codes) (Bogdan and Biklen, 2003). The coding process is defined by Strauss and Corbin (1990, p. 3) as "*the analytical process through which data are fractured, conceptualized, and integrated to form theory*".

Our data analysis of our first round of interviews took place in five stages. After contacting possible participants, we conducted the interviews with the 35 large French organizations in French, and then we fully transcribed them. The transcribed text was categorized into different themes (codes), we analyzed the coded categories, and finally we translated them to English for the purpose of this research dissertation. The data analysis is represented in the following Figure 22.

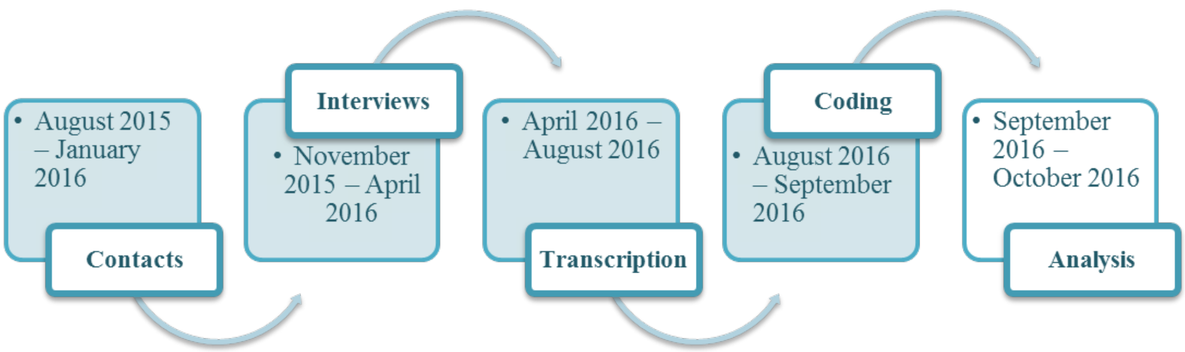


**Figure 22: Phase I – data analysis stages**

The fully transcribed interviews along with the notes taken during the sessions were coded using the software Nvivo, version 11 (Phase 4 of our data analysis). The analysis was guided by a critical, self-reflecting and skeptical perspective as suggested by Elliott and Timulak (2005). We started by dividing our data into distinctive meaning units: units communicating sufficient information for the reader even without the context (Elliott and Timulak, 2005). In a first round of open coding, we identified numerous codes to which we assigned different text fragments. As reasons behind adopting/not adopting cloud solutions emerged from this coding process, we used the categories gained from the literature review (i.e. the benefits and risks of adopting cloud solutions) as seed categories for this theme and then assigned the lower-level codes into these broader categories, as suggested by Elliott and Timulak (2005).

For example, a quote by the participant IT.2,

*"Implementing cloud solutions for various usages scares us. The questions 'once you are in the cloud, how will you get out of it', and 'how to change CSPs if we need do' concern us",*

was open-coded with 'concerns' and later assigned to the category 'reversibility'. To illustrate further, if we consider a quote mentioned by the participant IT.1,

*"In the year 2000 we had 44 platforms and 66 information systems. Today, we find our IT department with 4 platforms and only one information system. We also aim at reducing that number to 2 platforms in 2 to 3 years."*

This quote possesses much information. First, it reveals the way the IT department is transforming through reducing their numbers of IS and platforms. Therefore, the first round of coding we assigned it to 'IT department transformation'. We, then, open-coded it to the category 'impact of cloud computing' and the sub-category 'internal transformations'; addressing the different transitions the organization has witnessed due to their cloud adoption.

In addition, IT.5 mentioned,

*"Today, the IT employees whose jobs were to parameter mainframes cannot use the same skills to deal with cloud services from Amazon for example. These are different logics and different competences."*

Whereas this shows the shift in the role of the IT department, it was assigned, during the second round of coding, to the ‘education of employees’ sub-category (category: impact of cloud computing). Moreover, even though categories (and sub-categories) mostly emerged inductively, our research question and literature review influence the thematic inductive process.

After coding all the transcriptions and notes into different categories, we analyzed them in Chapter 4. In addition, we wanted to study the link between IT governance and cloud maturity of organizations. Therefore, the following section represents the second round of interviews conducted for this purpose.

## 4.2 Phase II - Second Round of Interviews

### 4.2.1 Data Collection

The data analysis of the first round influenced the development of a second round of interviews. The aim of this section is therefore to study a potential link between implementing effective governance when adopting cloud solutions and the intensity level of cloud adoption in the organizations (cloud maturity). To do so, we conducted a second round of interviews with the same organizations, but with a structured format. While our 35 participants have advanced knowledge in business and IT subjects, with degrees from a prestigious school, and high levels of experience, we judged them capable of assessing the cloud maturity level of their organization.

The interview guide in this round was well prepared before starting the interview, where it was based on the questions of Table 12 in Chapter 2 (section 5.3). Thus, during our second round of structured interviews, we directly asked the participants all the questions from Appendix II. As represented in Table 12, cloud maturity is assessed through 18 questions, regarding 8 domains (business strategy, organization and skills, governance, projects, architecture, operations, infrastructure, and information). During each interview and for each question, our purpose was for the participant to assess the maturity of their organization by choosing the appropriate maturity level (from CMM1 to CMM5). For example, we started with the question *“Does a formal enterprise level strategy exist positioning the use of cloud based services?”* in the **Strategy** domain. We proposed the 5 possible answers, each one corresponding to a level of maturity. The participant then assessed their organization by choosing an answer from the 5 possible ones. For instance, IT.16 chose *“Yes, but with ad-*

*hoc adoption*" answer, corresponding to a CMM2 for this question in the **Strategy** domain. We followed the same steps for the rest of the questions and for all of the interviews.

It is also important to state that the second round of interviews helped in increasing the validity of the emerging results from the first round. Participants agreed that they had to go through modifications of their IT governance before adopting cloud computing. For instance, their current IT governance mechanisms are insufficient to govern cloud technologies. This led to implementing decision-making structures, business processes and relational mechanisms adapted to cloud services. Almost all participants agreed on the urgent need for updating employees' skills.

### 4.2.2 Data Analysis

Our data analysis for the second round of interviews took place in three stages. We started by contacting the same participants again, asking them for a possible second round of interview with close-ended questions (from November 2016 till January 2017). We then conducted a second interview with each participant to collect the needed empirical material (from January till March 2017). Finally, we analyzed the collected data (April and May 2017). The data analysis is represented in the following Figure 23.

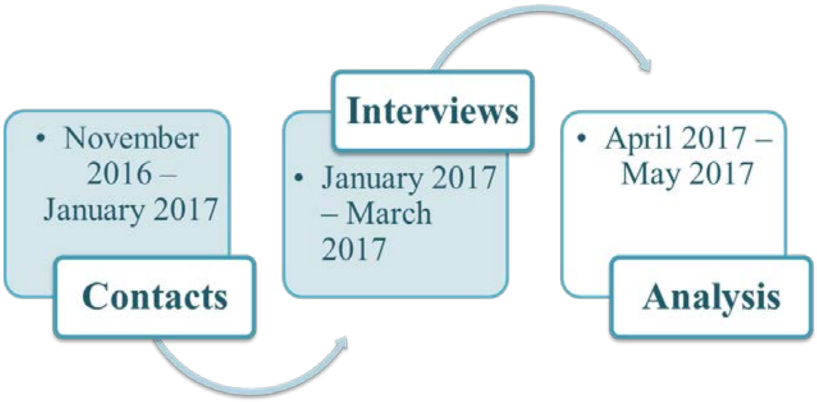


**Figure 23: Phase II – data analysis stages**

After the participants chose one answer out of 5 for the 18 questions and hence, after they assessed the cloud maturity level of their organizations accordingly, we started the analysis phase. Since the cloud maturity is assessed in 8 different domains, we started by calculating the maturity level average of each domain, to then calculate the total average of the 8 domains, leading to the cloud maturity level of the organization. The purpose of calculating the average of each domain is to help organizations improve the domains lacking maturity.

After calculating the total average of each organization's cloud maturity, we had to classify them accordingly in one of the 5 levels (CMM1 to CMM5). The results will be presented in Chapter 4.

### 4.3 Documentation

In addition to our two rounds of interviews, we answered our research questions based on some documentation. Data collection occurred in several stages; while some documentation was collected in the pre-phase of the first round of interviews, others were collected during the step 1 of the data analysis of Figure 22.

As mentioned in Table 16, we first used additional empirical material from information received via alternating emails. When we were exchanging emails with potential participants, we received some information regarding their organizations to see whether they suit our research work. Moreover, during the interview process, some organizations provided us with additional documents regarding their organizational processes, missions, future plans, etc. In addition, we also based our research work on articles found online, or on organizations' websites.

To illustrate the different types of documents received, IT.7 showed us a board report stating the different transitions towards cloud computing, IT.14 provided us a document with the list of their cloud service providers and their services, while explaining their choices, IT.8 redirected us to whitepapers found online, IT.22 showed us the preliminary decisions towards the adoption of PaaS, IT.2 emphasized the strategy decisions mentioned in a board report, B.6 evoked the document stating the mission of their organization and their future plans, and finally IT.6 provided us with a document stating the different processes implemented by the organization (not solely related to cloud services).

The data analysis of these documents, in addition to the notes taken during the interviews, were taken into account during the analysis phase (step 5 of Figure 22) of the first round of interviews, via the software Nvivo. This secondary data provided us with additional information in order to contextualize the organizations and their routes towards CC.

# Findings

This chapter is divided into two parts. The first part is responsible for analyzing the 35 semi-structured interviews conducted with large French organizations, where numerous ideas arose. The second part constitutes the data analysis of the second round of interviews with the same participants, but possessing different aims.

The data analysis of both parts was guided by the tag cloud of the interviews represented in Figure 24. It was created by the software adopted for the data analysis – Nvivo v11 – and shows the mostly cited words by the 35 participants during the phase I of interviews. The words with the largest size in tag clouds represent the mostly cited ones. Therefore, the larger the size of the word, the more cited it was by our participants. As our interviews were conducted in French, the following Figure 24 represents a tag cloud of French words. We chose the most 150 cited words between our participants. The frequency of these words ranges from 1478 times for “cloud” to 19 times for “médias” (media). Appendix III illustrates the frequency of the 150 most cited words.


**Figure 24: Tag cloud from interviewed participants**

Several important words emerged in this tag cloud, such as, "données" (data), "métiers" (business departments), "gouvernance" (governance), "services", "sécurité" (security), "besoins" (needs), "changement" (change), "risques" (risks), "compétences" (competences), "transformations", "réversibilité" (reversibility), etc. The emergence of these words led to a deepened analysis regarding numerous subjects. This analysis will be presented in this chapter.

# Part I: Phase I of Interviews

The objective of this dissertation is to explore and understand the way cloud computing is perceived and governed in French large organizations. A number of important insights have emerged from the first round of our analysis.

The present sections portrays respondents' perceptions regarding cloud computing and its impact on organizations. It also highlights the perceived risks as well as benefits of cloud computing and presents the governance models that are implemented in French organizations.

## I. Cloud Computing and its Impact on Organizations

Business units as well as IT units share the same representation of cloud computing. This representation is mostly aligned with the definitions found in the literature. According to our participants, cloud computing represents the act of having professional organizations offer technological solutions (IaaS, PaaS, or SaaS) to any user without pre-requisites. Thus, cloud computing is viewed as a solution where everyone will be connected to it, even if it is just a black box for them (IT.2). These scalable and on-demand solutions enable users to exploit information in a packaged, organized, industrialized way, with performance and price guaranteed (IT.24, IT.23, B.9, IT.16, IT.22, IT.2). They are viewed as "*a pack of Lego where if demand increases, Lego parts are added, and similarly if demand decreases, Lego parts are removed*" (IT.24), a colossal rupture in "*the way information is stored and treated*" (B.9) and "*the way it connects people in different environments*" (IT.5). However, the adoption of cloud solutions is affecting organizations on different levels. Transitioning to the cloud is not an easy task on large organizations, "*it was hard for [the organization] to suddenly shift from a-one system on premise to the cloud. This is much easier for start-up companies for example*" (IT.14). Our respondents are witnessing transformations within the organization and the IT department. New roles, skills and stakeholders are emerging and gaining importance in large organizations where cloud services are being adopted.

## 1. Towards a more Business Oriented Approach

The adoption of cloud services has transformed the role of the IT department in large organizations. In traditional computing environments, the IT department was accountable for implementing IT services whenever needed, and prescribing them to business units without really consenting with them, "*this is what we will do, this is how we will do, and we are the only ones who will know how to do it*" (IT.16). In such environments, its role was to explain to the business departments the different digital issues faced by the organization, while emphasizing the security problems. It had complete control over the achieved services and products, imposing them on the business units "*even if these services are not a 100% in line with the business departments' needs*" (IT.5). Hence, the first aim of the IT department was to work within budget and time while delivering their products or services.

However, with the emergence of CC as well as with the increased competition in the digitized world, the focus on business needs and demands has been emphasized. This digital transformation is a business transformation where "*new business models impacted by new technologies are emerging*" (IT.12). Thus, the aim of IT departments "*shifts today towards being oriented to [the] business departments and using IT in achieving business needs*" (IT.8). Yet, this change of perspective has affected the role and goals of IT departments in large organizations. According to our interviewees, the role of the CIO diverged from handling IT infrastructure to a role where he is strategically involved in the business growth and product development. In addition, the number of IT services (architecture, networking, UNIX integration networks, Windows integration networks, etc.), previously provided by the IT department, has significantly decreased with the presence of cloud computing; "*IT departments do not have to deal with the daily infrastructure issues anymore*" (IT.16).

In today's environment, business units are able to adopt cloud services without even involving the IT department. Thus, the facilities and possibilities offered by cloud solutions have affected the power previously held by the traditional IT department; "*cloud computing deprives some power of the IT department*" (IT.4); "*the role of the traditional IT department will scarcely disappear*" (IT.20). As a result, the centralization of the IT department is no longer a necessity with the adoption of CC. Therefore, organizations are witnessing a shift in the sovereignty of IT where business departments act independently. For instance, as business departments are being contacted by several CSPs, they do not require the IT department for developing new applications. In addition, business departments (especially the marketing and communication departments) are very reactive to the organizational business ecosystem. While they are also very responsive to the market, they are always innovating and trying to find ways to influence the market. This pushes the IT department to be "*reactive in order to avoid being bypassed*" (IT.8). Therefore, it becomes fundamental that the IT department understands that its role is evolving from being "*prescriptive to proactive*" (IT.17, IT.16, IT.8, IT.14). CIOs should take into account the business department needs, be "*aware of how demanding clients have become in the digital age*" (B.6) and "*require [their] validation on each stage of creating an application*" (B.5). In addition, the IT department has to be "*up-to-date on the different approaches and technologies available in the market*" (IT.8) in order to offer "*better strategies and solutions*" (IT.17). This will help both business and IT departments to "*co-construct*" IT solutions, "*we build together whenever we see the emergence of a new technology, or whenever we think we can do things differently, so we work on improving our processes*" (IT.5); "*we are really immersed in the co-construction between our business and IT departments*" (IT.13). Moving towards the idea of "*building everything together*" (IT.13) is essential to maintain a visibility on what is being developed, bought from a provider and adopted; "i*t is very dangerous that the IT department is losing its power and control over the organization's IS*" (IT. 19).

## 2. Emergence of New Skills in IT Functions

The integration of CC affects the activities of employees in the IT department, "*old jobs are disappearing and giving places to new ones*" (IT.12), as well as the required skills, "*employees need to develop new skills that match with the new job*" (B.6). With the evolution of the CIO role and the need to constantly adapt to business evolving needs, the acquisition of business knowledge becomes necessary "*CIOs, particularly, should not only be satisfied with their IT knowledge, but they should expand it and earn some business knowledge as well*" (IT.5). It is preferable to have CIOs with a "*cocktail profile; good knowledge in IT and business at the same time*" (IT.2). Our interviewees insisted on "*having CIOs with mixed profiles in the near future to match with this digital era*" (IT.15). As the IT department is no longer just a service supplier, "*it participates in the business arbitration while having a minimal technical knowledge*" (IT.2). This orientation is vital because even though CIOs are working from the technical angle, "*they are also involved in the business side of the organization*" (IT.15). IT functions need to be proactive and aligned with business strategies in order to survive in today's digitalized organizations "*the CIO's role would be to provide flexible and agile solutions as the ones found in the cloud, in order to fulfill the various business needs in an agile way*" (IT.16). Thus, the emergence of cloud computing has led to changing the hiring criteria of IT people as well as the training program content. IT people are advised to go through several trainings in order to understand the emerging technologies and better manage it in their organizations. Some of our respondents admitted their need to hire graduates that are "*business and IT oriented, with some data privacy knowledge, in order to fit in [their] IT team*" (IT.15). It is very rare and hard to find graduates with all these skills together, along with good reflexes regarding security, data privacy, and data management. Furthermore, many of our respondents evoked the need of evolving the IT degree program to this digital era by integrating IT-oriented as well as business-oriented knowledge "our *education system that is not quite adapted to the digitalization of today's society*" (IT.5), "*universities need to adapt their classes and teaching methodologies to the digital transformation*" (IT.16).

Besides business and IT employees, syndicates are the groups of people of the organization that are the most threatened by the integration of cloud computing. They try to oppose the organization from adopting cloud solutions. However, even threatened, the IT department is not always on their side. For instance, during their meeting with the syndicates, some advised them to "*listen to the radio, watch TV, read the newspapers and most importantly to be updated about today's society*" (IT.2). Even if they know that objecting to cloud solutions is not the best for organizations, "*they still try to oppose in order to save their seats*" (IT.16). Moreover, due to the ubiquitous characteristic of cloud solutions, employees can work anywhere, allowing them to avoid coming to the office every day. However, the labor law in France revolves around the number of hours spent in the office. This classic vision does not match with today's digital vision. Therefore, syndicates will hardly accept the switch from hours spent in the office to the content of the work done. This is an important social switch in France to which syndicates still strongly oppose, making it imperative to "*educate syndicates on this evolution*" (IT.16).

## 3. New IT Processes, Methodologies and Infrastructure

Data findings highlight changes in the organization's processes, its infrastructure, as well as in the project management methodologies.

Transforming processes is part of the digital transformation affected by the implementation of cloud solutions. According to our respondents, organizations "*have been working on structuring their processes*" (IT.3) in order to have more automated and lighter processes. Due to the automation and to the adaptive solutions brought by CC, methodologies and structures are changing. The agility of cloud solutions is transforming the organization's processes into more agile ones (IT.5, IT.12, IT.24). Thus, the development cycles have become shorter, departments are exchanging more often, and the IT department is more rapidly developing solutions that better respond to business needs. The agility brought by cloud computing "*has impacted the different departments of the organization*" (IT.13). Therefore, organizations are starting to evolve one step after the other, where "*at each step they will draw a conclusion then pass to the next step*" (IT.8). With such agile processes, organizations are becoming more "*automated, dynamic, elastic, and quickly detecting threats*" (IT.15). The agility brought some changes in the way organizations begin dealing with the encountered problems. For instance, once project teams stumble upon an incident, they wonder how quickly, in their next step, they should fix the incident faced in production, instead of just rolling back. This method corrects errors faster than actually backtracking. It changes most of their "*pre-established models*" (IT.5, IT.9). Moreover, with the adoption of cloud technology, roles that are more agile have naturally emerged in IT departments as well as new skills have become necessary. While some organizations created the role of scrum masters, "*Scrum master should be directly present when [the organization] is dealing with agile processes. He facilitates the integration of agile methodologies. When [the organization] first adopted SaaS and IaaS solutions, [it] immediately saw the need to introduce scrum masters to guide the employees with the agility*" (IT.8), others created "*small structure called The Lab, which is responsible for developing applications, faster and in a more agile way*" (IT.13, IT.16). The role of cloud services is, hence, extremely important in achieving agility in large-scale projects. In order to become agile, "*breaking [their] traditional organizational models is a must*" (IT.5).

Data findings also highlighted that the digital transformation is affecting the organization's infrastructures (IT.11, IT.12, IT.5, IT.7, IT.13, B.4). Organizations are questioning their infrastructures; whether to develop internal applications or adopt public cloud services. Traditionally, the infrastructure world regrouped people "*familiar with physical infrastructures, such as installing servers, installing routers, connecting cables and* *configuring the different parameters*" (IT.22). However, when organizations implement their infrastructures in the cloud, they would modify some parameters by simply sitting on their desktops. Additionally, deploying public cloud solutions offers various benefits for organizations, as they "*do not have to worry about all the technical side*" (IT.11), and where the 'cloudification' of the organization is turning its "*physical assets into software services*" (IT.13). It is bringing the organization to a virtual world, where the different elements have become virtualized. For instance, some organizations are "*switching from a closed internal infrastructure*" (IT.7), "*to an open and scalable one through adopting PaaS and IaaS solutions*" (IT.5). Therefore, moving to cloud computing is not a hard task, technically, as long as the organization is "*well engaged in the virtualization where most of [its] servers are virtualized*" (IT.12) – which constitutes one of the first steps of the transition.

## 4. New Approaches of Security and Data Privacy

The digital transformation is also affecting the security monitoring and data privacy of organizations adopting cloud services.

Historically, with the presence of the legacy, security teams monitored the organization's security through conducting different security tests, including "*vulnerability assessments and network penetration tests*" (IT.22). Nevertheless, when adopting cloud solutions, security teams should ensure the "*reliability of the contracts agreed upon with the CSPs*" (IT.16). For instance, they should monitor that these contracts "*cover all the required standards of the security aspects of cloud solutions*" (IT.11). Thus, instead of technically monitoring and verifying the security of cloud services through tests, their role is "*shifting towards contractual monitoring*" (IT.8).

In addition, data privacy is being considered as one of the most important organization's assets. This new extra value for data is an important change brought by the emergence of cloud computing. Data leaks also triggered the importance shed on such assets. After different data leaks incidents, organizations realized that their data have a sacred value and hence it needed to be highly protected.

Many participants agreed on the importance of data privacy in a cloud environment, and shared their experiences. For instance, the clients' data for utilities organizations are extremely valuable. If competitors stole these data, with the consumption history of each client, they will earn a competitive advantage. These data encompass the payment history, their solvability, the different ways of payment, the type of consumption, the usages, the number of electrical machinery home, their addresses, etc. They will then be able to "*prospect these clients leading the organization to the edge of bankruptcy*" (IT.11). This exaggeration shows the importance of data privacy in their organization. Whenever organizations want to adopt cloud solutions from different providers, In fact, "*organizations should spend a large amount of time on their contracts with the different Cloud Service Providers especially regarding the Data Privacy clause*" (IT.8). In addition to the contract clause, organizations also should hire a data privacy officer – if they do not have one already – in order to monitor the organization's data. The data privacy officer is responsible for "*going through all of [their] projects to ensure a data flow convenient to the norms set by the different countries – when the organization has several branches all over the world*" (IT.5). IT.5 explained that whenever the data spend one millisecond in France, "*it must be compatible with the norms set by the CNIL – Commission Nationale de l'Informatique et des Libertés*" (IT.5). Plus, whenever it is related to the infrastructure, it is important to "*evaluate the CSPs compliance with some key points regarding their data security*" (IT.2).

Other interviewees focused on the importance of data privacy in their sectors, such as the railway sector, which is a state market with public governmental money paying to build the infrastructure, through public operators. The most powerful governments of the world – USA, China, France, Germany – consider "*the railway construction a strategic industry, which is why, it is prone to advanced spying at the state level*" (IT.3). Therefore, they try to secure their data by avoiding storing them in a public data center, which will be directly accessed by the NSA (National Security Agency). Data privacy is a very important concept for several sectors (IT.1, IT.2, IT.3, IT.9, IT.19). IT.1 also added that they have a private cloud with their own data center, where they store all of their data, and share them with other social protection entities, in what they call a 'trust bubble'. They have secured sharing processes between their different entities, leading to private and secured data (IT.1).

## 5. CSPs: New Stakeholders in Organizations

Among other changes that cloud computing has brought to the organizations, interviewees evoked the relationship with cloud service providers (CSPs). For instance, the relationship with providers was almost absent for large organizations during the legacy, except for organizations that used to outsource their IT processes. Data findings show that some organizations witness the creation of a relationship with their CSPs since the emergence of cloud computing, which was not quite mentioned in the literature.

As CSPs are part of the cloud computing ecosystem, organizations agree that they cannot implement public cloud solutions without building a relationship with their CSPs (IT.2, IT.3, IT.9, IT.10, IT.22). They noticed a strong relationship built between their "*IT department*" (IT.2) as well as their "*business departments*" (IT.3), and their CSPs. In addition, in order to get public cloud services, organizations need to sign "*legal contracts with the appropriate CSP*" (IT.16). Therefore, legal contracts link the organization with its appropriate CSPs. A solid relationship between them is "*primordial*" (IT.22) when adopting these solutions.

Even though such relationships are primordial and necessary, organizations are skeptical about choosing their CSPs due to security issues. Thus, benchmarking appears to be essential for organizations to "*cautiously choose trustworthy providers*" (IT.9). This is a vital step knowing that the "*contracts are not signed for a short period of time*" (IT.16).

## 6. The Development of Shadow IT Practices

The adoption of cloud solutions seems to enhance the adoption of software and services that are outside the ownership or control of IT departments. This can lead to increasing costs and risks in organizations. Our data analyses show two groups of organizations: ones that fully control their budgets and do not allow any trace of shadow IT and others that are witnessing many shadow IT activities.

### 6.1 Organizations with No Sign of Shadow IT practices

Few interviewees mentioned that shadow IT does not occur in their organizations. These ones have a common point: they are centralized and the IT department is in control of the development and implementation of IT services (IT.1, IT.2, IT.5, IT.6, IT.8, IT.9, IT.10, IT.13, IT.16, IT.17, IT.19, IT.20, IT.21, IT.23). In such organizations where the IT department is centralized, the budgets are highly supervised. The IT department monitors the contract documents in order to stay in control of the activities happening in the organization. As long as the IT department is centralized, the others need to respect it and have its agreement before buying any cloud solution. Hence, "*business departments do not have the budget to buy solutions from CSPs*" (IT.6) and they "*need to ask [them] before taking any* *decision regarding the implementation of cloud solutions*” (IT.9). In addition, “*when it comes to [their] core IT, business departments cannot short-circuit the IT department to avoid putting the entire IS at risk*” (IT.1).

## 6.2 Organizations with Shadow IT Practices

According to other groups of interviewees, shadow IT is present in their organizations (IT.3, IT.4, IT.7, IT.11, IT.12, IT.14, IT.15, IT.18, IT.22, IT.24, B.1, B.2, B.3, B.4, B.5, B.6, B.7, B.8, B.9, B.10, B.11). Our data analysis shed light on several points regarding shadow IT, including why it occurs, for which service models it occurs, and its impact on IT departments as well as organizations.

### 6.2.1 Reasons behind Shadow IT Practices

Shadow IT occurs when business departments short-circuit their IT department to adopt cloud solutions from CSPs. Data findings evoked the presence of “shadow IT” in the organizations when business needs are not correctly fulfilled. When the IT department is decentralized and where the notion of power does not exist, the business departments have more freedom and more budgets to contract with vendors when they need a cloud solution. In addition, business departments usually deal with short specific deadlines to deliver a product or a service. However, when these people realize that their IT department does not have the appropriate solutions to accomplish their projects, they get frustrated and decide to seek help elsewhere. They turn towards cloud service providers and decide to short-circuit their IT department. They would prefer implementing a cloud service in few days than waiting two months to install a virtual machine with the hassle from the legacy. In some cases, when business departments are not satisfied by the time taken to implement the demanded services, they nag on to the CEO who caves in and gives them some budgets to buy cloud services. Moreover, shadow IT mostly occurs due to cloud service providers communicating directly with the business departments. IT.3 explained the way shadow IT happens: CSPs usually come to the organization to talk with the business departments, avoiding any contact with the IT department. They try to persuade them with their offers, luring them into a 3-month contract at first. After these trial months, CSPs automatically renew contracts with the business departments who have not meticulously read the signed contracts. Meanwhile, the IT department is being short-circuited and paying monthly bills.

### 6.2.2 Which Service Models are Mostly Concerned?

According to our analyses, shadow IT is mostly seen with SaaS solutions (B.10, B.8, IT.11, IT.12, IT.4), where business departments act independently of their IT department. At some point, these departments will be willing to see directly the CSPs and buy SaaS solutions without involving the IT departments in their decisions. Therefore, in order to avoid this incident, B.6 advised "*the IT department to take the initiatives and be proactive*". It should be closer to the business departments, learn about their different needs, and achieve them within budget and time and through new services and innovative technologies. When the IT department is not being able to provide a good service, it should understand the need for shadow IT for IaaS. For example, when "*the communication department needs to store 50 Terabytes of video files, they inform their IT department that it is bugging on the internal infrastructure*" (B.8). Hence, they search for a CSP that could offer them large storage capacities with a good quality of service.

### 6.2.3 Shadow IT Impacts on IT Departments and Organizations

Data findings share different opinions regarding the impact of shadow IT on IT departments power. On one hand, some agree that cloud computing has brought a "*new power for business departments through shadow IT*" (B.11) and the "*IT department is losing their control and power over the organizations, [the organization] is witnessing a gradual shift towards decentralization*" (B.8). On the other hand, others state that "*even through buying offers from CSPs, business departments come asking for [the IT department's] help*" (IT.12), and arguing that "*even if these are cloud solutions, [they] do not know how to use them, and [they] need [the IT department's] guidance*" (IT.3). Regardless of the presence of shadow IT, "*the IT department should not slow the business departments down*" (IT.22); on the contrary, it should "*put them on the right track, guide them and help them take steps forward, in order to avoid threats*" (IT.4).

Additionally, some interviewees focused on the risks generated by shadow IT in their organizations. For instance, business departments think they can bypass the IT department and buy solutions directly from CSPs. However, they are unaware of some legislation issues; some countries do not allow their data to be stored outside their territories. Therefore, when business departments are not compliant with the legislation of their countries, they get involved in several serious issues. In addition, some "*do not pay full attention to the CSP trustworthiness, the quality of their services, and particularly to the security issues*" (IT.11) even if "*the IT department tends to make the business departments aware of the risks brought by shadow IT*" (IT.18). It is the IT department's job to verify all these aspects, which cannot happen when business employees short-circuit them. Therefore, when shadow IT happens with recklessness, it is severely dangerous and harmful to the organization. In addition, shadow IT can start with small costs that keep on adding and reach a larger amount. For example, IT.3 affirmed that "*[their] IT budget last year was 80 million euros and jumped to 140 million euros when [they] added all the shadow IT activities*". The financial department plays an important role in monitoring the business departments' budgets in order to avoid such surprises. Moreover, small expenses are not traceable, "*although [they] control 1000 applications, [they] discovered 2000 applications from shadow IT*" (IT.3). Therefore, the IT department cannot monitor all expenses, which makes shadow IT easily implemented.

Table 18 summarizes various explanations of the absence and presence of shadow IT activities in the interviewed organizations. Some organizations do not witness shadow IT activities due to the total control of their IT departments on one side and the full assistance and collaboration provided by their IT departments on the other side. However, the majority of organizations have seen shadow IT activities and explained it under different angles. First, several participants agreed that the root of these activities is the business departments' evolving requirements. In addition, others mention that shadow IT activities allow the shift in power from the IT to the business side, creating a new dynamic within the organization. However, while some highlights the high risks engendered by such activities, few evoke the assistance and efforts shown by the IT department in order to help business departments in using the adopted services.

**Table 18: Shadow IT under different angles**

| | | |
|---|---|---|
| Absence of Shadow IT | IT control | - "*Cloud providers make us laugh as they come to our organization and try to convince the business departments to buy their solutions, not knowing that the business cannot sign any contract without our agreement*." (IT.2)<br>- "*Business departments do not have the budget to buy solutions from CSPs*" (IT.6)<br>- "*Business departments need to get the [IT department's] permission before seeking solutions from cloud providers*" (IT.10) |

| | | |
|---|---|---|
| | | - *"[The IT department] controls everything related to software, solutions… really anything related to IT."* (IT.19)<br>- *"[Business departments] are not allowed to go behind [the IT department] and contact cloud providers.*" (IT.20) |
| | Collaboration | - *"We do not witness a lot of shadow IT. We're more the discussion-kind of organization, where business come talk to [the IT department] about a new need.*" (IT.24)<br>- *"No, I don't think shadow IT is a huge problem in our organization. This is so because of our policies, stating that we build together with the business department, so if they need anything, we are here for them.*" (IT.8) |
| Presence of Shadow IT | Departments Needs | - *"I can say yes, it is present in some parts of our centralized organization based on some departments' urgent needs. Let me stress on the word urgent.*" (B.3)<br>- *"Even if the governance is centralized, business departments have tried short-circuiting the IT department. Mostly when the provisioning duration takes too long, but [the business departments] do not have enough budgets.*" (B.7)<br>- *"Well shadow IT is a bit complicated to explain and to defend. Business departments are moving fast, with more work and shorter deadlines, due to the fast-moving market. So it is understandable that they get the solution the minute they need it.*" (B.9)<br>- *"I think that regardless of whether [business departments] do short-circuit the IT department, it should not slow them down. I mean it's normal that they will not be able to fulfill all sorts of needs today, especially with all the offers provided out there.*" (B.5)<br>- *"We do buy solutions from providers; I will give you an example. When the communication department needed to store 50 Terabytes of video files, they informed the IT department that it is bugging on the internal infrastructure. So since it was bugging a lot, and they had deadlines, they searched for providers offering large storage capacities and a good quality of service.*" (B.8)<br>- *"We mostly buy software solutions from providers; they don't usually cost a lot of money to the organization, but here as a senior project manager, I'm only talking about my department.*" (B.4) |
| | Shift in Power | - *"We feel that the business departments want to possess new powers through the cloud, and specifically through shadow IT. But they do not possess a high budget to buy software"* |

| | | |
|---|---|---|
| | | (B.2)<br>- *"I do feel that the IT department is no longer in total control of the organization. Especially with the presence of all the different cloud solutions offered by providers.*" (B.11)<br>- "*Even when buying offers from CSPs, business departments come asking for [the IT department's] help. So even if we witness some shadow IT actions, our expertise is still required*" (IT.12) |
| | Risks generated by Shadow IT | - "*Yes [business departments] do short-circuit [the IT department]. It is dangerous. Shadow IT is really dangerous. Especially when our business departments do not pay full attention to the CSP trustworthiness, the quality of their services, and particularly to the security issues*." (IT.11)<br>- "*During a meeting with our IT department, we discussed the consequences of shadow IT present, and the ways to reduce it. It turned out that our IT department tends to make the business departments aware of the risks brought by shadow IT. This does not seem to reduce it though*." (B.10)<br>- "*Our business departments have a very small budget to buy software that is not harmful. Other than that, with our centralized nature, [the IT department] does not allow them to get risky solutions*." (IT.4) |
| | Assistance from IT department | - "*The IT department tries to take the initiatives and be proactive to avoid shadow IT where our business departments need specific software.*" (B.6) |

As a summary, data analysis presented several different findings. First, as they are adopting cloud solutions, most organizations remark a transition in the role of their IT department, along with a shift of power from their IT departments over to the business ones. Although some focused on the need of developing skills and education, others emphasized their internal transformations (processes, infrastructure, methodologies, and security testing). Moreover, organizations witness an addition to their lists of stakeholders – CSPs. Finally, CC seems to also affect the data privacy of these large French organizations as well as the creation of shadow IT activities in a large number of them.

# II. Corporate Strategy behind the CC Adoption

Cloud solutions are not implemented just for fun. Every organization has a motivation for adopting them. Three main corporate strategies have been identified throughout our data analysis: the highly market competition, the urge for innovation, and the reduction of costs.

## 1. The Highly Competitive Market

When asked about the motivation, some organizations stated that they are implementing advanced cloud services due to the competitive market (IT.16, IT.7, IT.5, IT.24, IT.8). *De facto*, what differentiates an organization from another, specifically today, is the way it deals with its information systems. While the organization's IS encompasses their adoption of cloud services, the organization needs to focus its attention on the way it deals with CC, in order "*to beat competition*" (IT.16). Competition depends on the industry, where in some cases it is accentuated. For instance, competition is high in the telecommunication industry. Hence, as a telecommunication organization, as noted by IT.16, in order to keep its clientele, their organization is motivated by competition to implement sophisticated cloud services. The High-Tech industry seems to be competitive as well, where organizations offering creative and innovate products can be easily replaced by another more mature organization. Therefore, such organizations "*need to stay up-to-date not to vanish with the extremely competitive market*". IT.7 explained that "*the new start-up that emerged with the cloud, stole many of [their] market shares*". Therefore, they decided to get involved more seriously in cloud solutions in order to regain their places in the market and win back the lost market shares. This competition helped the organization strive for a better cloud adoption. For other organizations, "*cloud solutions pushed [them] to have many opportunities that [their] competitors have*". They continued that this left them at the same level of their competitors, "*and it is up to [them] to reach a higher level*" (IT.5).

## 2. The Urge for Innovative Solutions

Other organizations stated that their strategy of adopting CC was its innovative aspect. Cloud computing is seen as an innovation for several organizations (IT.12, IT.3, B.9, IT.14, IT.11, IT.18, IT.15, B.6, B.10, IT.23, B.8, IT.17, IT.9, IT.10, IT.20, IT.19, IT.2). For instance, they base themselves on cloud solutions to "*create faster more innovative IT services to satisfy [their] customers*" (IT.15). The utility industry is evolving, where innovative products and services are being implemented. Therefore, utility organizations are basing their innovation on cloud solutions and they are "satisfied" (IT.11, IT.12, IT.14). The innovation side of CC triggers public organizations as well. With CC, a public organization can implement a "*strategy that is focused on their citizens while working with modern tools*" (IT.19). CC is just a "*modern innovative tool that organizations need because it is 2016*" (IT.20).

### 3. Reduction of Costs

In addition to competition and innovation, some organizations evoked that their strategy was the reduction of costs (IT.22, B.11, IT.15, IT.2, IT.4, B.4, IT.21, IT.13, B.8, IT.6, IT.17, B.5, IT.1, B.1, B.2, B.7, B.3). Their objective is to reduce their costs, motivating them to adopt cloud solutions. Before adopting cloud solutions, organizations tend to analyze their costs. For instance, through the costs analysis, cloud computing allows the organization to "*identify and classify better [their] costs*" (IT.6). In addition, after discussing it with their business departments, "*in order to analyze the different costs reduction generated by CC, [they] discovered that such solutions will decrease their total costs*" (IT.4). This pushed them to move towards cloud technology. These organizations aim at reducing their total costs, through "*minimizing the total costs from adopted tools on-premises, in addition to maximizing [their] reduction of costs from adopted cloud solutions*" (B.5). Moreover, even public organizations are tempted by the reduction of costs as long as their data are secured; "*Whenever a data center in the French territories will be available, allowing [the organization] to evolve with total security while reducing [their] costs, [the organization] will be the first to store [its] data there*" (IT.1).

Therefore, our participants have different strategies for adopting cloud solutions. While some are interested in keeping their market shares and not losing their clientele, other focus on the innovation side of CC. Finally, some organizations are tempted by the reduction of costs generated by cloud services. It is also interesting to notice that some organizations mentioned more than one strategy, meaning that they based their cloud adoption decisions on two motivations (for example, IT.15 "*along with the innovative side of the cloud, [they] also take into consideration the reduction of [their] costs*", IT.17, IT.22, IT.2, B.4, and B.8). In fact, the motivations mentioned by our participants highlight the urge for aligning IT with business strategies. Thus, it is fundamental that IT departments collaborate with business units in order to better understand the market needs and anticipate the right innovative solutions that would meet these needs.

# III. Benefits of Cloud Computing

While the strategies behind adopting the cloud vary, large enterprises are turning to cloud services because of its associated benefits. Data findings identified several benefits of adopting cloud solutions. Organizations deploying cloud services experience improvements in organizational economics, scalability, performance, agility, ubiquity, and standardization.

## 1. Economic Benefits

The ‘pay-per-use’ or “on-demand service” characteristic of cloud computing enables organizations to buy services and capacities for as much time as needed. Several Over-the-Top organizations provide cloud solutions and service maintenance that are much cheaper than buying the needed machinery, and internally developing and maintaining the needed solution. The difference in “*price between a license solution and a cloud solution*” (IT.23) is clear in the market. Cloud computing is at a tipping point for a large number of organizations.

In addition to the cheap solutions, cloud computing allows a lower electricity consumption. Adopting cloud technology will be “*much cheaper than internally providing the same services*” (IT.12). Moreover, when organizations “*do not possess virtual machines or servers to turn on and maintain*” (IT.11), they are also saving money through a lower electrical consumption. Some also viewed cloud computing as a green energy where less physical equipment is plugged in (IT.12, IT.11, IT.16).

## 2. Scalability Benefits

The scalable characteristics of cloud computing has also been cited as very beneficial for private and governmental organizations. .

The advantage of cloud computing is its light structure due to its flexibility. Several agreed that this flexibility is sought in today’s fast-growing market (IT.3, IT.12, IT.11, B.11, IT.14). Instead of buying capacities from the start – as done traditionally – “*cloud computing allows [organizations] to scale up and down according to [their] needs*” (IT.3). *De facto*, scaling up means “*the possibility to quickly order an increase in resources*” (IT.11). In addition, the term cloud computing was metaphorically represented by IT.7 as "*being an elastic cloud and having the capacity of deploying infrastructure as needed according to peak-loads*".

According to our respondents, the scalability and flexibility characteristics of cloud computing "*solve the problem of deploying solutions throughout all the different entities*" (IT.2) for organizations with a complex architecture. Instead of deciding to provide infrastructure, or provide environments for tests and deployment, they touch the complete system, by scaling up and down.

The scalability characteristic is also beneficial for governmental organizations that deal with applications for an unpredictable number of citizens, "*the ability to easily scale up and down as desired*" (IT.19). Additionally, IT.9 also agrees and explains the benefit of using cloud solutions as they implemented a new service for citizens, "*We were unsure of the number of citizens that we are going to use this service on our website. We couldn't forecast the number of citizens; it could have been either 200 000 people or 3 to 4 million people*" (IT.9). However, implementing infrastructures for 3 million people is very different from implementing ones for only 200,000 people. Therefore, the scalability and flexibility offered by cloud solutions pushed them to deploy their new service on the infrastructure of a trustworthy CSP located in Europe.

### 3. Performance Benefits and Improved Quality of Service

Another benefit associated with the integration of cloud services is the increased performance in organizations. As mentioned in the literature, cloud technology offers simplified operations, good service quality, and robust machines. These qualities increase the organization's performance. Our interviewees also agreed with this benefit. Cloud services are more energy-efficient than traditional IT services. Thus, organizations implement such solutions for the optimization of their resources, the high Service Level Agreements of providers, and the increased quality of their services.

Our data revealed the way cloud computing helps organizations optimize their resources. Traditionally, organizations "*used to buy servers and then install them*" (IT.12), a very time-consuming technique. However, organizations never used all their servers' capacities, leading to "*a waste of time and money*" (IT.16). Therefore, cloud computing has created an agile infrastructure benchmark, that is more performing than traditional techniques. For instance, cloud service providers are linked to the concept of provisioning, where they offer a service the moment organizations demand it. Organizations, hence, do not buy servers since all the chain is already provided by the cloud service provider.

Moreover, Service Level Agreements (SLAs) are important when deploying cloud services. SLAs represent a contractual agreement of the level of the services offered by the CSP. Organizations seek the highest SLA possible, since a higher SLA leads to a lower servers downtime. An SLA of 99.0% means there will be a 1% downtime during the year, equivalent to 3 days, 14 hours and 24 minutes a year[30] (almost 15 minutes per day). As small as this amount might seem, losing almost 4 days a year is costly for successful organizations. Nevertheless, Over-the-Top providers promise in their contract an SLA of 99.95% leading to a downtime of 0.05% per year, equivalent to 4 hours 19 minutes a year (43 seconds per day), which is acceptable. "*There are thousands of servers in the CSPs datacenters that go down daily*", explained IT.22. A technician is daily present to replace those servers. However, the performance of these servers is related to the CSP's promised SLA – it depends whether it is a downtime on average of 40 seconds a day or 15 minutes a day. This pushed organizations to adopt cloud services from Over-the-Top providers in order "*to optimize [their] performance and lower [their] downtimes*" (B.5). In addition, shifting some applications to the cloud "*decreases [the organization's] batch treatment from 15 to 20% while increasing the availability of services from 92% to 98.6%*" (IT.24). This would have "*never been possible with internal applications*" (IT.24).

Additionally, data findings highlight the quality of cloud services. For many argued reasons, "*large actors that fully depend on their reputations and quality of their services trust cloud solutions*" (B.9). Some participants elaborated by illustrating with some examples, on the way cloud solutions increased their performance. For instance, IT.19 gave us example of the increased performance of some cloud services their organization deployed. They stated, "*The aim of deploying cloud solutions is to facilitate the approaches citizens have on our website, while renewing their passports, consulting their driver's license points, etc. This facilitated the citizens' approaches and exchanges between administrators, in addition to having a more successful and performing public service*" (IT.19). In addition, our participant IT.22 fortified

[30] SLA calculation from: https://www.netways.de/en/support/tools/sla_rechner/

their argument with the example of a popular service operator, Netflix. This rising organization is dependent on the quality of services it offers. It thus, switched from an internal deployment to a cloud environment offered by a trusty CSP with high promising SLAs.

Finally, IT.14 explained that they evaluated their organizational effectiveness, through distributed employees' and clients' surveys based on the KPIs, regarding the use of cloud solutions. Through this evaluation, they noticed a "*visible increase in organizational effectiveness*" (IT.14).

## 4. Agility Benefits and Decreased Time-to-Market

The implementation of cloud computing results from a long decision-making process where cost benefits associated with the integration of these solutions is assessed. According to our participants, "*cloud solutions have more effects through increasing the agility of [their] processes rather than reducing [their] costs*" (IT.13). With its agile aspects, cloud computing pushes the different departments to communicate and work together in order to create projects together.

Due to the automation brought by cloud technology, methodologies, structures, and the governance seem to be affected. The agility of cloud solutions is transforming the organization's processes into more agile ones. The development cycles have become shorter, departments are exchanging more often, and the IT department is rapidly developing solutions that better respond to business needs. The agility brought by cloud computing "*has impacted the different departments of the organization*" (IT.1). Therefore, organizations are starting to evolve step by step, where "*at each step they will draw a conclusion then pass to the next step*" (IT.15). In other words, organizations are starting to work in an iterative way. With such agile processes, organizations are becoming more "*automated, dynamic, elastic, and quickly detecting risks*" (IT.16). In addition, the increasing agility brought some changes in the way organizations start dealing with the encountered problems. For instance, once they stumble upon an incident, they stop the production in order to figure out a solution that fixes the encountered incident. Thus, by enhancing closer relationships between different departments, cloud computing is helping organizations change most of their "*pre-established models*" (IT.7, IT.13).

In addition, the adoption of cloud services helps organizations decrease their time-to-market "*we are being able to adopt transformations much faster than if we had to do them internally*" (IT.10) and "*implementing platforms internally would take us longer than simply adopting cloud services*" (IT.12). Time-to-market is an important concept in today's fast-changing society. Due to the agility of cloud computing, projects have a lower time-to-market. Data findings reveal that organizations experienced a decrease in their time-to-market due to the increased agility of their processes. They stressed on the fact that they deploy cloud solutions "*when [they] need to access resources in a real-time manner*" (B.3), and "*when [they] lacked time for some development projects, [they] had to use cloud solutions in order to get real-time results*" (IT.7). Agility for some participants (IT.16, IT.7, IT.20, IT.6) means that "*what used to take [them] 6 months or even 2 years with [their] traditional IT, takes 2 or 3 days with the adoption of cloud services*" (IT.16).

Additionally, cloud solutions encourage organizations to continuously integrate and deploy "*we have several deployments per day*" (IT.16). Along with the agility, cloud computing supports DevOps principles. This emerging concept values continuous and permanent development and improvement, over short period. Data findings evoked the presence of DevOps in organizations due to the agility of cloud solutions (IT.22, IT.7). Cloud solutions are extremely compatible with the DevOps approach. In order to become agile, organizations need to migrate technologically, searching for technologies allowing them to develop faster, cheaper, and to continuously integrate as well as deploy. However, "*breaking [their] organizational models is a must in order to become agile*" (IT.7).

## 5. Ubiquity Benefits

The ubiquitous nature of cloud computing has made it very popular among organizations. Due to the mobility of cloud solutions, users can access their resources at any time, in any location.

Cloud computing is helping organizations solve many issues related to their geographical distribution. For instance, when a large organization possesses thousands of devices around the world, "*the only solution to deal with Mobile Device Management is through having it stored in a cloud*" (IT.2). In addition, when distributed employees need to share an updated document, "*the fastest solution is to save it in the cloud*" (IT.2), where these employees will access it immediately. In addition, in complex organizational structures, the ubiquitous characteristic of cloud computing is perceived as an added-value "*storing all data and* *documents in the cloud where employees can use them, is an added value for [their] work*" (IT.13). Cloud computing seems to be an effective solution for reducing costs and facilitating work in disturbed environments "*we did not want to go through the trouble and work of hosting our mail services. It takes a lot of time hence we decided that adopting ubiquitous cloud solutions, with low monthly costs, is the right solution for our organization*" (B.5).

While an important added value of cloud computing is its ubiquity, interviewees also highlighted the ease of accessing data. The ubiquity of cloud solutions increase employees' autonomy since "*hardware is transformed into a logistic asset transported everywhere*" (B.11). In addition to the ergonomic and high quality of the simulation tools provided by CSPs, organizations are satisfied by the ubiquitous access of their documents (IT.9). This characteristic is also "*increasing the amount of people teleworking*" (IT.3), where their "*data is not only available at work but at home as well*" (B.5). Moreover, the fact that information and processes are not local anymore, yet shared across the network "*facilitates all of [their] work*" (B.4).

## 6. Standardization

### 6.1 Benefits

Even though only few participants commented on the standardization of cloud services, this characteristic seems to be perceived as a positive aspect. While most of the reviewed studies considered this aspect of the cloud as a negative one, affecting the competitiveness of organizations and limiting customization, our participants viewed it as an advantage for organizations. According to them, the standardization aspect of cloud computing enables Over-the-Top providers to offer solutions at lower costs, which is a trigger for many organizations (IT.3, IT.11, IT.15) "*the more specific the solutions are, the higher the costs*". Furthermore, some expressed their satisfaction with the standardized virtual machine they are renting from a trustworthy CSP (IT.11, IT.15), where "*buying specific cloud services induce higher costs*" (IT.11).

### 6.2 Standardized Solutions and Competition

In order to survive in today's competitive environment, organizations thrive to get assets that differentiate them from their competitors. Thus, considering the adoption of standardized cloud solutions as a competitive advantage is questioned by numerous studies and practitioners. However, data findings show that organizations who are adopting standardized solutions can demark themselves from competitors in several ways.

Some interviewees stressed on how cloud solutions can support their manufacturing and way of doing in order to gain a competitive asset (IT.3, IT.13) "*differentiation happens through the way we design the overhead lines, the pantograph, and the cost of manufacturing a railway; Cloud solutions help us in that"* (IT.3).

Others focused on the important role that the marketing department plays in demarking its organization's business from others'. Even if all organizations adopt the same SaaS solutions, their usages and services can be different. The key point is to have an innovative marketing department capable of delivering, through standardization, personalized solutions for the final client (IT.16). Thus, understanding client needs and being able to address them, with the help of standardized cloud solutions, would create an added value for the organization.

Some participants also mentioned that standardized cloud solutions increase their capacity to quickly develop products/services that differentiate them from their competitors (IT.11, IT.2). In this respect, organizations can customize the quality of their products and services and demark themselves from their competitors even if they are using standardized cloud solutions. However, organizations should not confuse 'differentiating themselves from others' with 'reaching the same level of competition as others'. For example, UBER is a start-up company that offers carpooling services or private taxi rides for a low price. Therefore, as mentioned by one of our interviewees, "*in a society where UBER has gained fast popularity, taxi companies should seek being on the same level as UBER instead of caring about differentiating themselves*" (IT.2).

Table 19 summarizes the various benefits perceived by our participants. We illustrate these benefits by drawing on quotations mentioned by some of our participants.

**Table 19: Cloud benefits perceived by participants**

| Category | Benefits | Quotations |
|---|---|---|
| **Economic** | - Pay-per-use characteristic<br>- Low electrical consumption<br>- Low prices | - Difference in "*price between a license solution and a cloud solution*" (IT.23)<br>- Cloud computing is being considered as a green energy (IT.12, IT.11, IT.16).<br>- Several cloud solutions are free of charge |

| | | |
|---|---|---|
| | - Disappearance of updates costs | (IT.3).<br>- "*Leave these applications and their updates to the cloud, where silent-versioning exists*" (IT.3). |
| **Scalability** | - Scaling up and down dynamically | - "*The possibility to quickly order an increase in resources*" (IT.11).<br>- "*Having the capacity of deploying infrastructure as needed according to peak-loads*" (IT.7). |
| **Performance** | - Optimization of resources<br>- Higher SLA leads to lower servers' downtime<br>- Quality of cloud services | - Traditionally, organizations "*used to buy servers and then install them*" (IT.12), which is very time-consuming.<br>- They adopt cloud services from Over-the-Top providers in order "*to optimize [their] performance and lower [their] downtimes*" (B.5).<br>- "*This has led to facilitate the citizens' approaches and exchanges between administrators, in addition to having a more successful and performing public service*" (IT.19). |
| **Agility** | - Agility of processes leading to a better risk detection approach<br>- Lower time-to-market<br>- Supporting DevOps approaches | - Organizations become more "*automated, dynamic, elastic, and quickly detecting risks*" (IT.16).<br>- "*When [they] lacked time for some development projects, [they] had to use cloud solutions in order to get real-time results*" (IT.7).<br>- Cloud computing helped them implement new approaches such as continuous integration, continuous development valued in DevOps approach (IT.22). |
| **Ubiquity** | - Ubiquitous access of data anywhere, anytime and anyway | - "*Data is not only available at work but at home as well*" (B.5).<br>- "*Facilitates all of [their] work*" (B.4). |
| **Standardization** | - Satisfaction with standardized CSPs offers | - Satisfaction with the standardized virtual machine they are renting from a trustworthy CSP (IT.11, IT.15). |

# IV. Risks of Cloud Computing

As it has been pointed out by our interviewees, cloud computing seems to benefit their organizations. However, important barriers and risks have been also identified in our data analysis. According to our participants, cloud services generate risks related to security, reversibility, compliance, society, and dependency on suppliers.

## 1. Security Risks

Data findings show that French organizations are unanimously aware of the security issues related to cloud computing. Our respondents emphasize the vigilance of French organizations in storing sensitive and critical data in public cloud due to security issues, confidentiality as well as sensitivity of data. This risk is even more highlighted in governmental organizations; "*adopting public cloud solutions is not the best choice especially for governmental organizations"* (IT.1). Interviewees are aware of the need of protecting their organizations from outsider attacks and data loss *"customers' sensitive data are extremely valuable*" (IT.9). While we cannot afford having outsiders attack our system, security is our main preoccupation (B.3). Large competitive organizations "*cannot tolerate the smallest security slip*" (IT.13). In addition, "*even with the presence of contracts*" (IT.8) that protect organizations' data, there is a "*risk of these data being consulted or retrieved by hackers*" (IT.4). Thus, participants agree that organizations need to display a higher level of caution when dealing with sensitive data (IT.12, IT.20, IT.9, IT.10, IT.19, IT.1, IT.21, B.3). For instance, the incident that happened in Japan few years ago, where the total retirement data of Japanese was lost, costed the Japanese Prime Minister his job. In addition, governmental organizations are also "*highly cautious on having [their] data leaked*" (IT.10). In fact, there are several laws imposing the governmental organizations to have "*full control of [their] sensitive data*" (IT.19) since cloud computing is not secured enough.

Data loss has become a major issue that needs to be taken seriously in order to stay competitive; "*If our critical applications fail us and we lose all of the data, related to our customers especially, we will be facing a huge complicated problem*" (IT.2). Our respondents show concerns regarding the way their data are saved "*we do not trust storing our data on the cloud to avoid losing them*" (IT.10), "we *do not know if our data are well saved*" (IT.12), or "*if we are going to lose them*" (IT.15). Thus, keeping "*strategic and critical data on our* *private cloud*" is considered by some organizations as a potential solution to this problem (IT.2).

Other participants focused on the image of their organization that will be affected by any data loss, data hacked, or data leaked (IT.6, IT.8, IT.22), although not mentioned in the literature. IT.6 explained, "*As a large financial institution, we have several governmental secrets that need to stay protected*". In addition, they have an image of trust, reliability and soundness, which is very important to maintain. Therefore, it would be very problematic for their image if the data were hacked. This pushed them to implement their "*private cloud due to the security issues found in the public cloud, especially affecting [their] image*" (IT.6).

Security issues in cloud computing appears to be a big threat for both private and public organizations. This problem seems to be even bigger when using public cloud solutions. Thus, although many efforts have been deployed in order to overcome this threat, organizations' data being loss, hacked or leaked remain a problem for many.

## 2. Reversibility Risks

Along with what has been reviewed in the literature, reversibility is considered as a major risk of cloud computing.

According to our interviewees, organizations mostly hesitate to adopt cloud solutions due to the reversibility issues (IT.17, IT.15, IT.20, IT.12, IT.19, IT.10). They wonder "*once [they] are in the cloud, how will [they] get out of it*" (IT.3). Therefore, some organizations have kept full autonomy on some strategic domains. In addition, the reversibility issue emerges with the dependency of organizations on their CSPs. The more CSPs have a large market share, the more they will impose their contracts and conditions on clients. While CSPs can afford losing few clients, the latter cannot afford losing their providers due to reversibility issues "*we need to deal with reversibility, which is a complex issue when we are dependent of third-parties and our data are located in a cloud environment*" (IT.20).

While cloud computing has been present for the past decade, organizations are starting to face their first reversibility issues. Due to the novelty of the concept, some predicted reversibility but miscalculated it at the start of the contract. Therefore, the moment they decided to move to another CSP, they discovered that the clause was "*not quite clear*" (IT.11). It is common to find organizations adopting PaaS solutions from a certain cloud service provider and hence, deploying applications written in a language specific to that provider. Consequently, the organization "*cannot recover its applications or install them with a PaaS solution from another provider*" (IT.12).

However, our data analysis highlights some optimistic opinions regarding the risk of reversibility. Few participants showed their optimism regarding the reversibility of cloud solutions. According to them, organizations should focus on the benefits of cloud computing while disregarding the reversibility issues. From our interviewees perspective, even though the business departments decide to switch to another cloud solution, "*it is not a big deal, they should just be aware that they might not recover all data*" (IT.2). In addition, according to IT.11, "*it is not very costly to move from a standardized and up-to-date virtual machine to another*".

## 3. Compliance Risks

Compliance issues are inevitable risks for organizations adopting public cloud services. Data located in public clouds need to abide by national and supranational laws as well as regulations. Data findings show the importance of locating the French organizations' data on national territories, especially when it comes to governmental organizations. *De facto*, the number of private organizations adopting public cloud is higher than the number of public ones. Public organizations aim at protecting their citizens' data which "*forbids [them] to store [their] citizens' data in servers located outside [their] national territory*" (IT.1). In fact, when an organization is in an international cloud environment and its CSP mentions that his servers are located in a certain country, the data thus follows the country's laws. For instance, the Patriot Act[31] is an act set by the USA government, allowing the American government to access freely the integrality of the data hosted in the USA. In addition, storing data in China means accepting "*the fact that these data will be intercepted and accessed by the Chinese government*" (B.10). Several interviewees were concerned with the location of their data being "*outside the Euro zone*" (B.3) where they will have to abide to the other countries laws.

Organizations, hence, want to find a regulatory way to protect themselves due to the recent issues (IT.1, IT.19, IT.9, B.10, IT.15, IT.12). Throughout the years, several regulatory acts

[31] http://www.olcu.org/PDFs/USPatriotAct_Summary.pdf

have been applied. A common act mentioned by a large group of our interviewees is the "*Safe Harbor*" (IT.12, IT.15, B.10, IT.19, IT.9). 'Safe Harbor'[32] represents the agreement of transferring data between the USA and European countries. This agreement was invalidated by the European Justice court in October 2015. After the invalidation of the Safe Harbor, organizations "*did not know how to safely transfer data between the USA and Europe*" (IT.8); therefore, they sought more costly and less practical solutions. This continued until the validation of the EU-US Privacy Shield framework, in July 2016 – which was not mentioned by our interviewees since it was validated after the period of the conducted interviews. *De facto*, The European Commission validated the adequacy of this framework to transfer safely transatlantic data. The CNIL passed a law stating that through the adoption of the Privacy Shield framework, French organizations can feel safer in transferring data, provided the organizations in the US receiving these data joined beforehand the register held by the American administration[33].

## 4. Societal Risks

As cloud computing generates transformations within the organization, it also generates social risks. The adoption of a new technology causes different reactions among stakeholders concerned by the use of this technology. Cloud computing has an impact on human resources, specifically of the IT department. Thus, people can feel uncomfortable with changing their way of working and dealing with daily issues. In addition, their jobs can be threatened by the introduction of cloud technology. IT.14 stated that their organization had to "*fire 200 employees whose skills have become obsolete*" (IT.14) one year after implementing cloud solutions (computing center). Managing employees is in fact highly affected by the emergence of cloud solutions. If the organization's strategy is to entrust its data to Cloud Service Providers, it does not really need its internal IT competences. IT.14 explained that they did not really need an IT engineer to manage payrolls in their organization. They have an account for a payroll management SaaS application at a well-known Cloud Service Provider, where they "*organized a basic training for few HR managers in order to manipulate the application interface*" (IT.14). Some participants evoked the hard task on their teams in

[32] https://www.cnil.fr/sites/default/files/typo/document/CNIL-transferts-SAFE_HARBOR.pdf

[33] https://www.cnil.fr/fr/le-privacy-shield

explaining to their IT employees that their jobs are ceasing to exist; "*it was the hardest part of the transition, the IT department was obliged to be entirely reorganized. The adoption of cloud services pushed the organization to seriously examine [their] IT governance*" (IT.16).

As outrageously mentioned by few interviewees, cloud computing is viewed as a mean to steal IT employees' jobs. Accordingly, cloud services should only be adopted when they are a necessity; "*after their 30 years of experience, [IT employees] affirm to [the CIO] that they are worried about being replaced by cloud solutions, hosted at an unknown location, with uncertain security, by people [they] do not trust. [The CIO] assures them it is not the strategy of [their] organization*" (IT.2). However, these employees should be aware that some services are too common and banal that the IT department do not intend to develop internally, since then "*it would not only be time-consuming, but costly as well*" (IT.6). It is normal to understand their reactions, when they have worked in the organization for several decades and have been involved in the evolution from the mainframe to the applications on tablets, "*they obviously see cloud computing as a threat*" (IT.2).

As our data show, cloud computing can decrease the number of staff in IT departments which can lead to people's resistance and reluctance regarding the changes brought by CC.

## 5. Dependency on Suppliers

The concept of dependency on suppliers was not mentioned in the academic literature. However, many interviewees talked about the high probability of CSPs controlling organizations, and thus making them dependent on their services.

It is important to notice that solutions offered by CSPs might seize to be available. Contracts link organizations to CSPs. However, when the contract of an organization with its CSP ends, the organization does not have any guarantee of the continuity of the cloud services. This makes it very dependent on its CSPs, putting it in a vulnerable position. The "*CSP can then manipulate*" (IT.5) the organization, by "*increasing the solutions prices*" (IT.6), for example. In addition, CSPs have their own roadmaps and "*they do not guarantee providing the same services on the long term*" (IT.14).

In addition, some might argue that organizations can audit their CSPs. However, while the CSP is usually the one providing the auditing tools to the organization, "*it has become extremely hard to fairly audit the CSP*" (IT.8). Therefore, as the organizations are using generic standardized solutions, they are "*completely dependent on the CSPs*" (IT.20), who tend to control them, where "*today, it has become critical to be dependent on suppliers*" (B.6).

Table 20 summarizes the risks associated to cloud computing as they are perceived by our participants. We illustrate each category with different quotations mentioned by some participants.

**Table 20: Cloud risks perceived by participants**

| Category | Risks | Quotations |
|---|---|---|
| **Security** | - Data Leaks<br>- Outsider Attacks<br>- Data Loss<br>- Organization's Image | - Governmental organizations are also "*highly cautious on having [their] data leaked*" (IT.10).<br>- "*Even with the presence of contracts*" (IT.8) protecting the organizations' data, there is a "*risk of these data being consulted or retrieved by hackers*" (IT.4).<br>- Keeping the "*strategic and critical data on our private cloud*" (IT.2).<br>- This pushed them to implement their "*private cloud due to the security issues found in the public cloud, especially affecting [their] image*" (IT.6). |
| **Reversibility** | - Vendor Lock-in | - "*Once [they] are in the cloud, how will [they] get out of it*" (IT.3).<br>- the organization "*cannot recover its applications or install them with a PaaS solution from another provider*" (IT.12). |
| **Compliance** | - Organization complied to national laws | - "F*orbids [them] to store [their] citizens' data in servers located outside [their] national territory*" (IT.1). |
| **Society** | - Need for education<br>- Firing policies<br>- Training sessions<br>- IT jobs being replaced/threat | - Organizations need to "*put a lot of effort and time educating employees and anticipating new needs*" (IT.11).<br>- Due to some firing policies of the French law, they are unable to fire them under the pretext that they lack skills adapted to cloud computing. It is "*one of the reasons [they] are not are fully immersed in the whole cloud universe*" (IT.6).<br>- They "*organized a basic training for few HR managers in order to manipulate the application interface*" (IT.23).<br>- When they have worked in the organization and |

| | | |
|---|---|---|
| | | witnessed the evolution from the mainframe to the applications on our tablets, "*they obviously see cloud computing as a threat*" (IT.2). |
| **Dependency on Supplier** | - Manipulation of prices<br>- Service not guaranteed for the long term<br>- Impossible to audit CSPs fairly | - "*CSP can then manipulate*" (IT.5) the organization, by "*increasing the solutions prices*" (IT.6)<br>- "*They do not guarantee providing the same services on the long term*" (IT.14).<br>- "*It has become extremely hard to audit fairly the CSP*" (IT.8). |

## 6. How would French Organizations Mitigate their Risks?

Several cloud computing risks have been reported in the academic literature and were agreed upon by our interviewees. Thus, minimizing these risks has become one of the top priorities of IT departments and organizations. Our data analysis portrays different ways that organizations seem to use in order to mitigate the risks brought by cloud computing. SQL ingestion technique, encryptions, monitoring devices, security policies, centralizing the security system, and adopting governance framework are among the solutions that have been evoked by our participants to mitigate cloud risks. It is beyond the scope of this study to explain and describe each technique organization uses to mitigate cloud risks. We will limit ourselves to list these techniques as they were evoked by our participants

SQL ingestion technique has been cited as one way to detect and prevent SQL injection attacks. It detects intrusion attempts and blocks the way in. For instance, the organization notices that "*when a hacker is trying to send a thousand SQL orders, provoking a textual typing error, with a weird code, every 10$^{th}$ of a second, [they] get notified that someone is trying to get inside [their] systems*" (IT.8). Encryption is another way of mitigating cloud risks for organizations. In order to "*secure [their] systems and mitigate the possible risks, we implemented several encoding streams and encryptions*" (IT.11). This technique enables the system to search for the 'e-seeker' through the 'gateways' right after the client connects to his account via the website. Using the client's Single Sign-On, the system displays the client's data, then immediately erases them without leaving any trace behind. This way, "*[they] make sure that if hackers get inside [their] systems, they will not be able to steal [their] clients' data*" (IT.11). It is a very hard and complicated task to do, but "*it is [their] responsibilities, [they] are extremely vigilant about it, and [they] cannot proceed without this security and* *vigilance*" (IT.11). While some mitigate cloud solutions risks is through "*adopting monitoring devices aiming at fighting any sort of external attack coming from cloud*" (IT.12), other "*implement a security policy for cloud computing that includes, surveillance, good practices, and a lot of communication*" (IT.7). Another way to fight such risks is through centralizing the organization's security system. IT.6 changed their security systems as cloud solutions were being implemented. They had "*several security teams that included the security of databases of [their] systems networks, databases administrators, and directory administrators*" (IT.6). Security systems can also be centralized into "*one security team, meticulously monitoring our systems and mitigating risks related to cloud solutions*" (IT.6). This centralization collects all security forces into one system fighting a large number of attacks.

Another cloud risk can come from breaking contracts with CSPs. According to our participants, an organization can break its contract with a specific CSP for several reasons, including, switching to another CSP or being bought by another organization with different CSPs. However, when an organization breaks its contract with a certain CSP, it has to "*pay penalties for breaking the contract*" (IT.22). These penalties are highly costly which can put the organization at risk. However, if the organization was bought by another one, then this latter is sometimes willing to pay these penalties in order to free the organization. IT.2 illustrated this with a current example, "*X was bought by Y, and meanwhile X was adopting solutions from Z. However, Y and Z had several arguments; therefore X had to break its contract with Z. The penalty costs were $60 million that Y was ready to pay in order to 'free' X. Therefore, X started adopting cloud services from the CSPs of Y.*" This represents one way of solving risks related to breaking contracts.

Moreover, ITIL and COBIT frameworks have been also cited as potential ways to control and avoid cloud risks (B.6, IT.8).

As data findings show, organizations are aware of the major risks generated by cloud computing. Thus, several ways have been identified in order to deal with these risks and mitigate them. However, there's no generic framework that is adopted and tested by organizations in order to manage and control cloud risks. In addition, deciding what cloud solutions the organization should adopt and how these solutions should be adopted remains challenging for organizations. Many decisions need to be taken in order to successfully integrate cloud solutions.

# V. Adopting Cloud Solutions: a Long Decision Process

## 1. Cloud Decisions

Shifting from traditional mainframes to implementing and adopting cloud solutions is not a simple task. Several decisions should be discussed and taken before immersing the organization in the cloud computing world.

Data analysis highlights a number of key decisions that organizations had to make before adopting cloud solutions. These decisions are illustrated by a number of questions stated by our interviewees.

While some organizations inquired about the use of cloud solutions with the question 'Why Cloud solutions?', others discussed the essential steps to transitioning towards CC. In addition, many questions evolved around cloud deployment and service models. When adopting cloud computing, organizations seem to focus on decisions related to data storage options, financial and security issues, required new skills. However, these questions are sometimes addressed as a part of the deployment and service model decisions. Few also mentioned decisions regarding cloud contract content, technical transition guideline, CSPs, policy options, and customers.

Table 21 categorizes the decisions that need to be made when adopting cloud computing. Each decision is illustrated by a sample of questions evoked by our respondents. It is important to precise that all organizations discussed the "Deployment model" and the "Service model" decisions. While some organizations focused on questions that deal with the strategic alignment between service models and business needs, others privileged questions related to cost reduction possibilities. Regarding the deployment model decision, organizations were mostly concerned about the security risks associated with the choice of the deployment model.

The decision process when deploying cloud services is critical as wrong choices can impact the organization. For instance, according to Tran and Bertin (2014), the choice of cloud service models (IaaS, PaaS, or SaaS) is a vital decision affected by the organizational model of the IT department (IS as a product, a service, or access). This emphasizes the importance of the decision-making process.

**Table 21: Cloud-related decisions addressed by participants**

| **Decision Questions** | **Quotations** |
|---|---|
| **Why Cloud Computing** | - "*Why are we adopting cloud solutions*?" (IT.22)<br>- "*We started wondering whether it solves the issues faced by our IT department, or does it just solve issues in theory*." (IT.2)<br>- "*We first wonder 'why do we need cloud solutions.'*" (IT.11)<br>- "*What is the trigger for using the cloud? Why can't we live without it*?" (IT.12)<br>- "*Over a long long long period of time, and during so many meetings, we discussed our need for cloud solutions*." (B.10) |
| **Transition steps** | - "*We need to lay down all the steps needed for implementing cloud solutions*." (B.6)<br>- "*Then we asked about the different steps to move to the cloud*." (IT.11)<br>- "*During our first meetings, we were wondering 'how are we going to transition towards the cloud*?'" (IT.24)<br>- "*We should consider what to restructure in the current organization to support cloud implementation*." (IT.5) |
| **Deployment models** | - "*Which cloud model does it add more value to the organization*?" (B.6)<br>- "*One of the first questions the organization asked was whether they implement cloud solutions internally or externally*." (IT.8).<br>- "*Is it best to start with our own private cloud*?" (IT.11)<br>- "*It took a while to decide whether we want to directly go towards a public cloud or just be satisfied by building our own*." (IT.23)<br>- "*I think, the first time we heard of cloud computing, we were very skeptical, knowing we are a public organization; especially after hearing about all these security threats, and breaches*." (B.1)<br>- "*I don't think we can ever trust the public cloud. It is an easy decision.*" (B.3) |
| **Service models** | - "*Which solutions do we buy*?" (B.9)<br>- "*What type of solutions should we get from providers*?" (IT.17)<br>- "*Which cloud service deployment do we adopt – IaaS, PaaS, SaaS? This is an important decision since it has an impact on the IT governance of the organization.*" (IT.22)<br>- "*Cloud computing is a huge new world. Deciding on software, platform, or infrastructure needed some time.*" (IT.21)<br>- "*Deciding on the cloud solutions we will be using in the next 5 years is hard to forecast knowing that our business departments tend to demand new specific solutions. Therefore, such decisions are made through the* |

| | |
|---|---|
| | *years."* (IT.6)<br>- "*I think we did spend enough time to decide on the type of solutions to adopt*." (B.7)<br>- "*Which cloud solutions are the most strategic for our organization*?" (IT.16)<br>- "*Which type of cloud can help us reduce our costs? We were wondering if we should just stick to software solutions or whether we can go further with some infrastructures*." (B.5)<br>- "*[The IT department] took a firm decision that only software solutions will be adopted*." (B.2) |
| **Data Storage options** | - "*In which domain are we allowed to adopt cloud solutions, and which domains are forbidden*?" (IT.3)<br>- "*What are the hosting possibilities on premises, on a public cloud or even on a private cloud*?" (IT.7)<br>- "*We make choices for the long term. It is crucial before implementing cloud solutions, to know which data we are allowed to put in the cloud*." (IT.6)<br>- "*What do we keep in our private cloud and what do we store in a public one*?" (IT.9)<br>- "*Due to our security policies, which data is allowed in the cloud? That is a primordial decision before going to the cloud*." (IT.10)<br>- "*Storing sensitive data in the public cloud was the fastest decision we made. We immediately rejected it*." (IT.19)<br>- "*As a public organization, we are not allowed to store citizens' critical data anymore other than on our premises*." (IT.20) |
| **Financial issues** | - "*An important question is related to financing cloud solutions. When an IT department buys a computing server, it is obvious that the IT department will be paying for it. However, when some department adopts cloud solutions, the financial question is not obviously answered. Therefore, it is important to ask ourselves which department will be paying for their cloud solutions.*"(IT.3).<br>- "*The reason we have a private cloud is because we analyzed the cloud solutions prices offered by Amazon, and we discovered that storing all our data on a private cloud on the long term, is cheaper than adopting Amazon cloud solutions*." (B.8)<br>- "*We noticed that adopting public cloud is only cost-effective in our case if we turned off the virtual machine half the time*." (IT.22)<br>- "*How will the cloud be funded? We had to do a cost/benefit evaluation in order to decide that*." (IT.16)<br>- "*We should also decide on our revenue model; will it be pay-per-use, subscription, etc*.?" (IT.14)<br>- "*Will the service provider ask for admission fees, and offer SLA* |

| | |
|---|---|
| | *compensation*?" (IT.2) |
| **Security Issues** | - "*It is important for us to solve the issues regarding the anonymization of our customers' data. As long as we cannot solve this issue, our customers' data remain in our private datacenters*." (IT.1)<br>- "*Which risks are we taking when storing these data in the cloud*?" (IT.5)<br>- "*Does the Cloud Service Provider guarantee the security of our data?"; "Are our data located in Europe or in the USA*?" (IT.11)<br>- "*We keep our clients' bank account details, for instance, the question here is 'who is allowed to consult these details, and who is allowed to modify them*? (IT.16)<br>- "*It is important for us to know the way to implement controls and map them to our processes to be able to mitigate potential risks*."(IT.8)<br>- "*How often should we track the progress of risk management activities*?" (B.9)<br>- "*Will our IT employees have to deal with other security issues*?" (IT.18) |
| **Required Skills** | - "*Will we need to fire employees whose skills have become obsolete*?" (B.6)<br>- "*I agree that training is very important. This decision did take part of our board meetings*." (IT.15)<br>- "*How many training sessions should we have per month to stay updated*?" (IT.7)<br>- "*We focus on training the employees since cloud solutions are not as easy as on premises solutions*." (IT.13)<br>- "*I think training employees is a must. The organization cannot be competitive if its employees lack major skills*." (IT.16) |
| **Cloud contract content** | - "*What are the contract restrictions with the cloud providers*?" (IT.16)<br>- "*We always wonder who is the best suitable group or team to agree on the contracts, before signing it with the providers*." (IT.5)<br>- "*Cloud contracts should be read seriously before any department signs it with the cloud providers, especially when shadow IT is occurring*." (IT.7) |
| **Technical transition guideline** | - "*While all the organization traditionally was on the same Operating System how can we adapt the different departments on different Operating Systems such as Linux, Mac, Windows*?" (IT.5)<br>- "*What technical guidelines must be used when adopting the cloud? What will change*?" (IT.16) |
| **CSPs choice** | - "*Which public cloud do we choose since costs and services differ between Cloud Service Providers*?" (IT.5)<br>- "*Why do we choose this provider over that one?', 'Which provider has the best client service approach that suits us*?" (B.9)<br>- "*A critical question is, 'Which cloud provider is on and off limits?' based on their reputations and the reputation of their solutions*." (IT.24) |
| **Policy options** | - "*What policies should we implement to adopt correctly cloud solutions*?" (IT.3) |

| | |
|---|---|
| | - "*Which policies are required for a correct implementation of cloud solutions*?" (B.6)<br>- "*We are still deciding on what kind of policies and procedures are extremely needed in our transition*." (B.11) |
| **Customers Relationship** | - "*How to maintain a good customer relationship*?" (B.4)<br>- "*Will we build more services to keep our customers satisfied, like online communities*?" (IT.4) |

Classifying these questions by decision types give us a clear picture of what needs to be addressed when adopting cloud services. An alignment between business strategies, organization critical needs as well as cloud computing decisions is necessary regardless of which decisions were made. Hence, different stakeholders should participate in the decision-making process in order to choose the appropriate cloud service and deployment models, as well as to better define the required skills, contract content, policies, etc. The section below portrays the cloud decisions makers that participate in the decision process when adopting cloud solutions.

## 2. Cloud Decision Makers

Data analysis evokes several different decisions makers related to cloud computing decisions. While most of the interviewees mentioned that the IT department is the primary decision-maker, others stated that different departments can also participate in the decision-making process of cloud computing. However, even when decisions are shared between the departments, one department tends to have the last call (whether it is the IT department (for example, B.1, IT.5, IT.7, IT.8, etc.), the board (IT.3), the financial department (IT.22), or the state representatives (IT.19)). This usually depends on who has the right information and the legitimacy to make the final decision.

In addition, the adoption of cloud computing seems to affect the decision-making process of certain organizations. While some have decentralized their IT decisions process "*the IT department made all of the decision up till the year 2014, where it shifted to a decentralization*" (IT.12), others moved "*to a centralized IT department in order to optimize resources and reduce costs while adopting cloud solutions*".

Table 22 illustrates the different locus of decisions along with the decision makers of all of our participants. It is important to note that the decision makers cited below (Table 22) are responsible for the cloud decisions mentioned above.

**Table 22: Decision makers related to cloud decisions**

| **Ref.** | **Locus of decisions** | **Decision Makers Related to Cloud Decisions** | **Quotations** |
|---|---|---|---|
| B.1 | Centralized | IT department | *"[The business departments] would like to discuss their decisions with the IT department, but it is the latter that makes the IT decisions."* |
| B.2 | Centralized | IT Department | *"[The organization's] governance is centralized, so it is the IT department that calls the shots."* |
| B.3 | Centralized | IT Department | *"When [the business departments] need a specific solution, they directly go ask the IT department, who will make the decisions."* |
| B.4 | Centralized | IT department | *"The business departments can't take their own decisions. They should transfer their wishes to the IT department."* |
| B.5 | Decentralized | Collaboration with arbitration from the IT department | *"[They] all discuss to choose the most appropriate solution/tool, but when it comes to the contracts of the CSPs, the IT department chooses."* |
| B.6 | Decentralized | Collaboration especially with the HR | *"When cloud computing has a social impact, it definitely has an HR impact. So the HR is part of [their] decision making."* |
| B.7 | Centralized | IT department | *"[The business departments] barely collaborate with the IT department. It is the IT department that makes all the IT-related decisions."* |
| B.8 | Centralized | IT department (some discussions with CEO) | *"It is the IT department, but [he CEO] also plays an important role in the process."* |
| B.9 | Decentralized | Collaboration with arbitration from the IT department | *"[Business departments] do discuss things with the IT department, but the IT department takes the final decision when [they] do not agree."* |
| B.10 | Decentralized | Collaboration with arbitration from the IT department | *"It is with the IT department that [the business departments] discuss and agree on the different cloud decisions."* |
| B.11 | Decentralized | Collaboration with arbitration from the IT department | *"Even if the IT department is the most capable and competent department to make such decisions, the cloud is "forcing" it to talk to business departments."* |

| | | | |
|---|---|---|---|
| IT.1 | Centralized | IT Department | *"Any decision that is related to our core IT, is only made by [the IT department]. So when cloud computing decisions need to be made, [the IT department is] the one deciding."* |
| IT.2 | Decentralized | Collaboration with arbitration from the IT department | *"It's between the IT and business departments, where these guys are certainly not inactive. Together, [they] build all the projects portfolios for example."* |
| IT.3 | Decentralized | Collaboration with an arbitration from the board | *"[The IT department] cannot impose a certain solution or a way to work on the business departments. [They] discuss the possible cloud solution and decide together. When [they] do not agree, the executive board is the one to take the final decision."* |
| IT.4 | Decentralized | Collaboration with arbitration from the IT department | *"[The IT department] is not the decision maker anymore, cloud computing deprives [it] from some power."* |
| IT.5 | Decentralized | Collaboration with arbitration from the IT department | *"Even if [business and IT departments] take decisions together, when [they] are not on the same side, [the IT department] arbitrates."* |
| IT.6 | Centralized | IT department | *"It is [the IT department] that takes the decisions, alone, without any discussion."* |
| IT.7 | Decentralized | Collaboration with arbitration from the IT department | *"[The IT department] tries really hard to keep this communication and discussion with the business departments so that they get fair decisions taken."* |
| IT.8 | Decentralized | Collaboration with arbitration from the IT department | *"There is a partnership installed in the organization between the IT department and the business ones, but it is the IT department that takes the last call when arguing."* |
| IT.9 | Centralized | IT department | *"[The IT department] takes such decisions."* |
| IT.10 | Centralized | IT department | *"The IT department is the only stakeholder in the decision process."* |
| IT.11 | Decentralized | Collaboration (all IT department of different subsidiaries) | *"[The organization] is constituted of different subsidiaries. Each one has its own IT department. So each one takes their own decision. Then, they all collaborate together."* |

| | | | |
|---|---|---|---|
| IT.12 | Decentralized | Collaboration | *"It is a collaboration, and especially regarding the infrastructure, and the SaaS solutions."* |
| IT.13 | Centralized | IT department | *"It is the IT department that should be the first to pronounce words such as cloud, big data, IoT. [They] should take the decisions related to these subjects."* |
| IT.14 | Decentralized | Collaboration | *"Collaboration is the key to success. When departments collaborate, better decisions are made."* |
| IT.15 | Decentralized | Collaboration (all IT department of different subsidiaries) | *"The subsidiaries of the organization take their own decisions first and then they all collaborate."* |
| IT.16 | Decentralized | Collaboration (all IT department of different subsidiaries) | *"It is different in [this] organization since [it] has many groups with [their] own CIO. So it is a collaboration of all of them."* |
| IT.17 | Decentralized | Collaboration with arbitration from the board | *"The IT department is not the only decision maker. It shares the decisions with the executive board, and based on the budget they take the decisions."* |
| IT.18 | Decentralized | Collaboration | *"Yes, [the IT department] collaborates with the business departments."* |
| IT.19 | Centralized | IT Department with accordance with Prime Minister | *"Once the Prime Minister gives us his OKAY, [the IT department] can then make the decisions official."* |
| IT.20 | Centralized | IT department | *"Yes, it is the IT department that makes the IT decisions alone."* |
| IT.21 | Centralized | IT department | *"The decision of [the IT department] is the only one that matters in [this] organization."* |
| IT.22 | Decentralized | Collaboration with accordance with Financial department | *"Decisions are made through collaborations, but first the financial department needs to approve in order to decide on the right cloud decisions."* |
| IT.23 | Centralized | Some collaboration; mainly the IT department | *"Yes it is a collaboration, but whenever [the business departments] needs a solution that [the IT department] does not want – due to security issues – it is [the IT department] that decides."* |
| IT.24 | Decentralized | Collaboration with arbitration from the IT department | *"[The IT department] meets with the business departments to discuss which solutions they need."* |

Even though many stakeholders seem to participate in the decision-making process of their cloud adoption, the IT department is cited as one of the primary stakeholders. Its advice and decisions are viewed as very important according to our interviewees. This can be explained by the fundamental knowledge and skills detained by the IT department when taking cloud-related decisions.

Despite the importance of the decision-making process, organizations need to govern their cloud solutions in order to control the cost, and make sure that these solutions are aligned with organization strategies and business needs.

## 3. Cloud Governance Mechanisms

Cloud governance mechanisms consist of decision-making structures, business processes, and relational mechanisms. Their aim is to work together, guide departments, and encourage them to a specific organizational behavior. Data findings highlight that organizations rely on several mechanisms when implementing cloud computing. While some of these mechanisms fall under IT governance in the literature, organizations use them while adapting them to the governance of cloud services. In addition, others adopt mechanisms that are specific to cloud computing.

The following sub-sections will display the structures, processes, and relational mechanisms helping organizations govern their IT with the presence of cloud services.

### 3.1 Decision-making Structures

A large set of structures is deployed by organizations in order to govern cloud solutions. These structures refer to the emergence of new roles within the organizations.

The emergence of the Chief Digital Officer seems to be crucial for organizations adopting cloud computing. In fact, the CDO is a person able to transform all the processes in the organization, the applications, as well as the internal and external relationships in a digital economy (B.11). The CDO is essentially, "*a CIO that has understood the way new technologies function*" (B.11), while trying to deploy these technologies correctly. The presence of the CDO pushes organizations to undergo transformations. His role is to help them through their digital transformation and transition. He aims at regrouping all departments, including the IT department and the general management, as well as "*helping* *them find solutions to the transformation issues they're facing*" (IT.8). According to our participants, the two departments that are mostly affected by this digital transformation are the marketing department, which will be attracted by new services, and the IT department, which is supposed to be developing these services. Thus, the CDO is "*the master of the orchestra*" (IT.16) pushing the business and IT departments to work together.

Our respondents also stressed on another structure: the IT steering committee. Even if these committees already exist in most organizations, their role seems essential for the implementation of cloud solutions where "*CC is part of IT projects*" (IT.15). IT steering committees, adapted to cloud technology, are responsible for monitoring reviewing and prioritizing major cloud projects through ensuring a continuous strategic alignment. In addition, data findings show that the creation of competency centers is important to help IT employees work together, share and coordinate their skills; "*[The organization] created a center of competency where 2000 IT employees work on the infrastructure, share their knowledge and coordinate their skills regarding cloud computing.*" (IT.11).

Participants also mentioned other structures, such as:

- Architecture Boards ("*a board that will provide you guidelines and advice regarding your architecture, knowing that CC will affect [the] organization's architecture*" (IT.22))

- Technical Architecture Committees ("*It actually represents a committee that meets regularly to discuss architecture standards when adopting cloud solutions. [The organization] aims at creating an architecture board in the near future.*" (IT.15))

- Chief Data Privacy Officers ("*It is like merging a Chief Privacy Officer and a Chief Data Officer in one job title, because both are extremely important for the protection of [the] organization's data. He will be first protecting the Data and guiding the organization through managing it well.*" (IT.5))

- Digital Project Manager ("*[the organization's] DPM is responsible for making things happen. This is a broad description, but his job consists on making things happen in the digital age, such as leading teams, empowering them and facilitating* *communication between [the different teams]. One can say that they are the architects of the digital age*" (IT.5))

- Chief Security Officers ("*The CSO may be one of the most important executives present in the cloud era. He needs to make sure that cloud policies are being developed, risks are being mitigated, and compliance is being applied."* (IT.16))

- IT Strategy Committees devoted for CC ("*This committee helps in identifying critical strategic issues faced when adopting CC, for example*." (IT.15))

- Purchasing Committees ("*[The] purchasing committee will discuss all the issues related to purchasing cloud solutions."* (IT.11))

- Legal and Technical Committees ("*It is an expert committee to deal at the same time with the legal and technical issues encountered since our organization started adopting public cloud solutions."* (IT.11))

- Chief Exchange and Digital Officers ("*A senior executive who takes care of all the exchanges related to mobile applications, the Internet, etc."* (IT.9))

- Data Management Committees ("*Such committees are self-explanatory; their role is to discuss the issues related to the management of [the organization's] data."* (IT.8))

- Having the CIO and CEO report to the Board of Directors

- Scrum Masters ("*A scrum master should be directly present when the organization is dealing with agile processes. He helps [it] facilitate the integration of agile methodologies*." (IT.5))

- Data Mining Experts ("*Such an expert is important for [our organization] to analyze our data and then turn it into valuable information, which then will be analyzed and turned into knowledge."* (IT.1))

Table 23 represents the major structures mentioned by our participants, along with some of their quotations. The focus of most organizations was on the introduction of a Chief Digital Officer (CDO).

**Table 23: Decision-making structures adopted by participants**

| **Type of Mechanism** | **Mechanism** | **Quotation** |
|---|---|---|
| Structures | CDO | - "*The CIO with the help of the CDO should be capable of correctly implementing cloud solutions*" (B.11)<br>- "*The CDO, however, possesses another mentality than the rest of the organization. He has a business expertise and is digital savvy*" (B.10)<br>- "*We have a CDO, especially responsible for monitoring our data*" (IT.19)<br>- "*The presence of the CDO in our organizations pushes us to undergo transformations*" (IT.16)<br>- "*New jobs are emerging with cloud computing, **CDO**, Chief Data Officer, Chief Security Officer*" (B.6)<br>- "*We have a Chief Digital Officer*" (IT.15)<br>- "*We have a CDO who is 95% business*" (IT.12)<br>- "*The Chief Digital Officer helps the organization through its digital transformation and transition*" (IT.8)<br>- "*We have a Chief Digital Office, who is the head of our strategy where our digital transformation is a strategic progress*" (IT.3)<br>- "*The CDO helps manage both teams, [the] IT department and the business departments*" (IT.24) |
| | IT steering committee | - "*An IT steering committee to govern data is also vital, where protecting data is highly important with cloud computing.*" (IT.16)<br>- "*We have an IT steering committee for the entire group where we decide on the different IT and cloud-related projects*" (IT.15)<br>- "*We have an IT steering committee*" (IT.7)<br>- "*We have steering committees for each IT project*" (IT.6) |
| | Center of | - "*We created a center of competency for IT*" (IT.12) |

| | | |
|---|---|---|
| | Competency | - "*Center of competency is primordial for centralized organizations with the emergence of new technologies*" (IT.8) |
| | Architecture Board | - "*Even if an architecture board is needed before the implementation of cloud solutions, it becomes primordial when [the organization] decides on adopting such services.*" (IT.22) |
| | Technical Architecture Committee | - "*We have a technical architecture committee constituted of the technical officers of the subsidiaries and focusing on the operational technical subjects*" (IT.15) |
| | Chief Data Privacy Officer | - "*New jobs are emerging with cloud computing, CDO, **Chief Data Privacy Officer**, Chief Security Officer*" (B.6)<br>- "*New jobs are being created by the digital transformation of [the]organization, including a scrum master, a digital project manager, **a chief data privacy officer**, a chief digital security officer*" (IT.5) |
| | Digital Project Manager | - "*New jobs are being created by the digital transformation of [the]organization, including a scrum master, **a digital project manager**, a chief data privacy officer, a chief digital security officer*" (IT.5) |
| | Chief Security Officer | - "*New jobs are emerging with cloud computing, CDO, Chief Data Privacy Officer, **Chief Security Officer***" (B.6)<br>- "*New jobs are being created by the digital transformation of our organizations, including a scrum master, a digital project manager, a chief data privacy officer, **a chief digital security officer***" (IT.5)<br>- "*As a telecommunication company, it is very critical to deal with secured data. So after many discussions, we judged that a chief security officer to deal with all the security issues of the cloud, is vital*" (IT.16) |
| | IT Strategy Committee | - "*The Strategic Governing Body meets every couple of months to discuss the evolution of the organization's strategy with the emergence of new technology – cloud computing for example*" (IT.15) |
| | Purchasing | - "*The Purchasing Committee collaborates with the IT department in order to manage all the important IT* |

| | | |
|---|---|---|
| | Committee | *contracts*" (IT.11) |
| | Legal and Technical Committee | - "*The Legal and Technical Committee deals with the usage of BIPS in order to store safely our clients' data*" (IT.11) |
| | Chief Exchange and Digital Officer | - "*We hired a Chief Exchange and Digital Officer who will take care of all the exchanges related to the mobile applications, the Internet, etc.*" (IT.9) |
| | Data management committees | - "*Data management committees are also important when dealing with a large number of Data*" (IT.8) |
| | CIO and CEO report to Board of Directors | - "*The IT department and the general management report to the board of directors*" (IT.7)<br>- "*We are making sure we report everything to the CEO who also reports them to the board*" (IT.16) |
| | Scrum Master | - "*New jobs are being created by the digital transformation of our organizations, including **a scrum master**, a digital project manager, a chief data privacy officer, a chief digital security officer*" (IT.5)<br>- "*We created a small structure called The Lab, which is responsible for developing applications, faster and in a more agile way*" (IT.1)<br>- "*After long discussion, and after seeing the agility of the cloud we decided to hire a scrum master to deal with the agility issues*" (IT.24) |
| | Data Mining | - "*There are new jobs created in the data mining field, including data sinks and data analysis*" (IT.1) |

Figure 25 represents a summary of the different decision-making structures that emerged from our first round of interviews, along with their roles in the organizations during the adoption of cloud services.

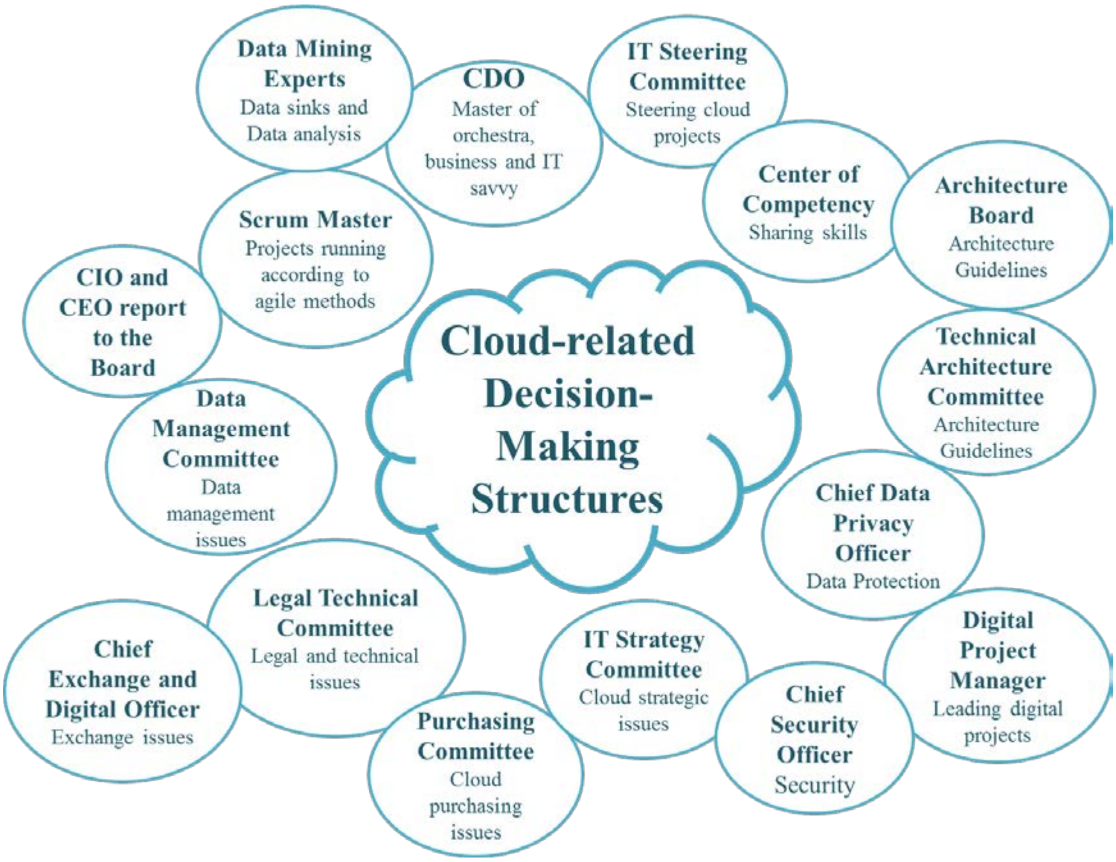


**Figure 25: Emerged decision-making structures for cloud services**

## 3.2 Business Processes

Even though processes play a major role in guiding the adoption of cloud solutions, only a few were evoked by our participants and highlighted in our data analysis. Organizations rely on IT governance frameworks such as COBIT, ITIL, ISO, and CMMI in order to govern their cloud. In addition, a few mentioned adopting scrum methodologies to deal with the agility enhanced by the adoption of cloud solutions. Only one participant added that its organization use balanced scorecards to support the business/IT alignment during the adoption phase. Table 24 illustrates the different processes adopted by the interviewed organizations when implementing cloud services. Even though some of the mentioned business processes were present before the adoption of cloud services, they are devoted to cloud computing.

**Table 24: Business processes adopted by participants**

| Type of Mechanisms | Mechanism | Quotations |
|---|---|---|
| Processes | Specific Processes | - "*We are developing our processes related to securing infrastructures and regarding our adoption of cloud solutions*" (B.11) |

| | | |
|---|---|---|
| | | - "*We are building our Cloud Policy that will instore the rules of the game in order to consume correctly cloud services. We started last year with frequent meetings to structure this cloud policy. It aims at educating employees about the security, costs and sustainability of cloud solutions*" (IT.3)<br>- "*We are transforming our internal communication processes in order to become more digitalized. We are already more digitalized, but we need to speed up the internal transformation*" (IT.15) |
| | Governance Frameworks; COBIT, ITIL, CMMI, ISO used with cloud services | - "*We use frameworks like COBIT and ITIL*" (IT.7)<br>- "*As frameworks, we adopt ISO and some of the functionalities of the ITIL*" (IT.6)<br>- "*We adopted an old version of COBIT. COBIT is mostly on the application side. In addition, ITIL is also a good framework*" (IT.12)<br>- "*Some ministries have adopted COBIT and CMMI framework with the emergence of cloud solutions; however, they did not maintain a conform and sustainable level*" (IT.20)<br>- "*We base some risks mitigation on the ITIL framework*" (IT.16) |
| | Agile/Scrum Methodologies | - "*We are mostly adopting scrum methods for their agile aspects*" (IT.12)<br>- "*With the arrival of the scrum master, we had to adopt scum methodologies*" (IT.5)<br>- "*Scrum methodologies are helping us in the cloud adoption process*" (IT.24) |
| | Balanced Scorecards | - "*What is helping with the agility of our processes is implementing Balanced Scorecards. These also allow us to follow our performance as we adopt cloud solutions*" (IT.7) |

As we can see, organizations lack unified processes to rely on in the adoption process of cloud technology. They draw on best practices found in IT governance frameworks and other IT project management methodologies and techniques. The lack of governance processes shows the immaturity of their actual governance when adopting cloud services. Figure 26 illustrates the small number of business processes adopted for cloud services by our interviewed organizations.

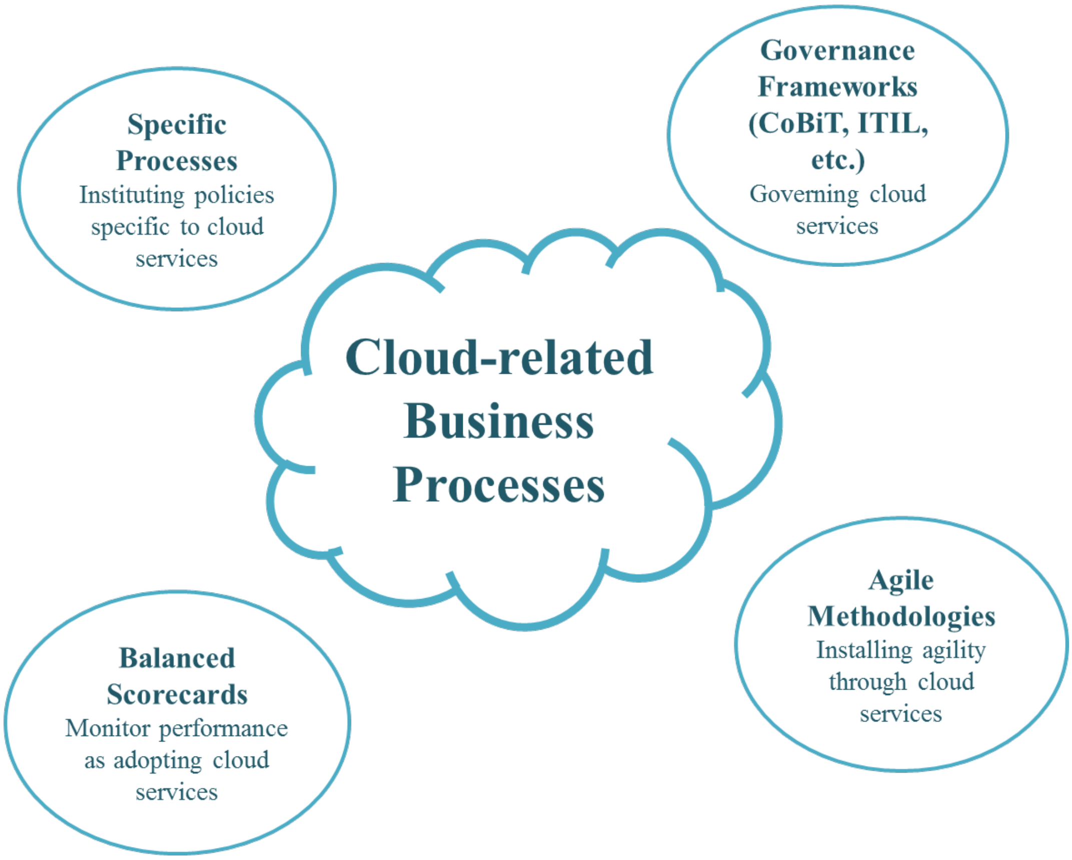


**Figure 26: Emerged business processes for cloud services**

## 3.3 Relational Mechanisms

Data findings stress the importance of relational mechanisms when adopting cloud solutions. The interviewees state that relational mechanisms are extremely vital for the governance of their IT, as they increase the synergies within the organization.

Table 25 shows the relational mechanisms mentioned by the interviewees when adopting cloud solutions. Communication and collaboration between the business and IT departments were the most mentioned mechanisms. With its agile aspects, cloud computing pushes the different departments to communicate, work together and create the project together. In addition, training and skill development seem necessary to use cloud solutions. Therefore, organizations have implemented numerous training and education programs for their employees in order to stay updated, learn the required skills, and develop new competences. In fact, organizations seem to be aware of the importance of conducting change when implementing new technology such as the cloud computing. While many organizations deployed awareness campaigns to educate their employees about CC, some offered them partnership rewards and incentives. Data findings also show that there is a shared understanding between business and IT departments. Finally, some participants evoked the importance of maintaining a good relationship with their CSPs, who became now part of the stakeholders' equation.

**Table 25: Relational mechanisms adopted by participants**

| **Type of Mechanisms** | **Mechanisms** | **Quotations** |
|---|---|---|
| Relational | Communication and closer relationship between business and IT | - "*We are trying to deploy more frequent meetings and shorter interactions aiming at being more agile*" (IT.19)<br>- "*IT is everywhere in our daily lives, where the interaction between business employees and IT is becoming more frequent*" (IT.19)<br>- "*Working together with the business departments created synergies between [them]"* (IT.9)<br>- "*We have different communities, such as Technology Front, Cloud Technologies, DevOps, which aims at increasing the exchange between employees* (IT.7)<br>- "*The IT and Business employees have been brought closer even physically, where they work together in the same OpenSpace*" (IT.7). "*Getting the IT interlocutors closer to the business ones makes the business evolve much faster*" (IT.7). "*The different teams communicate and exchange*" (IT.7)<br>- "*Resisting to changes does exist in [the] organization, but [they] take it as an advantage since it pushes [them] to communicate. When employees communicate, they produce fewer errors. Therefore, communication is extremely important when aiming at digitally transforming the organization*" (IT.6).<br>- "*During the cloud solution adoption phases, there is first a deconstruction of the relationship between the IT and business departments. However, this relationship is being reconstructed again due to integration and cyber security issues*" (IT.3). "*Even when [the] business departments bypass [the IT department] and buy cloud solutions from CSPs, they come back to [the IT department] asking for help to use these solutions. Hence, working together is a necessity*" (IT.3)<br>- "*For [the] organization, the relationships between the business and IT department are primordial. It becomes what traditionally was called a relationship between* |

| | | |
|---|---|---|
| | | *the project manager and the project developer*" (IT.1) |
| | Cross-functional business and IT job rotations and training | - "*In order to stay updated, [their] teams often follow trainings*" (IT.13)<br>- "*[The] engineers need to be trained every year to be updated with the latest technologies*" (IT.12)<br>- "*[The] IT department is trained, but [they] need to also train the business departments. When a highly used application is changed, they need to be accompanied in order to be able to use this new application" (IT.10).*<br>- *"[The organization has] a deployment plan that includes several training in order to deploy successfully this new type of cloud solutions*" (IT.9)<br>- "*[They] do sometimes prepare cross-functional trainings and [they] have some cross-functional job rotations*" (IT.7)<br>- "*[They] have some cross-functional job rotations related to digitalization, such as for project developments. However, the business departments have barely rotated jobs*" (IT.6)<br>- "*Sometimes [they] offer some cross-functional trainings for [their] employees to keep their skills updated*" (IT.24)<br>- "*[They] do have trainings for employees, but it takes a lot of time*" (IT.5) |
| | Awareness Campaign | - "*Awareness Campaigns are extremely important*" (IT.16)<br>- "*Business department should be aware of all the risks the organization would go through when adopting cloud solutions – legal risks, data risks, security risks, image of the organization. Therefore, awareness campaigns help the organization adopt cloud solutions more consciously*" (IT.8)<br>- "*When the whole cloud subject had emerged, and after studying its implementation, [the IT department] decided to spread awareness throughout the whole organization. It was also to share the newest updates across the whole organization*" (IT.24)<br>- "*Recently, we have been spreading awareness regarding cloud computing through implementing awareness campaigns*" (IT.7) |
| | Partnership rewards and | - "*Even incentives are prepared in our organization, pushing employees to be excited about this digital* |

| | | |
|---|---|---|
| | incentives | *transformation*" (IT.7)<br>- "*[The IT department] organizes contests, kaggle contests to be precise, every now and then. It is a contest where [they] give a challenge and data scientists and developers will try to solve the problem. This way allows [the IT department] to hunt talented IT people, having the required skills and hence hire them*" (IT.5)<br>- "*[The IT department] offers incentives. It is very important to keep [their] employees interested in the newest technologies*" (IT.24) |
| | Shared understanding of business and IT objectives | - "*There is an understanding and an alignment of the business and IT objectives*" (IT.7)<br>- "*One of the main objectives of [the] company is to keep [the IT department's] objectives aligned with the ones of the business*" (IT.16) |
| | Relationship with CSPs | - "*[The IT department's] relationship with the providers is quasi-new, but will be developed. [It] should maintain a good relationship with trustworthy cloud service providers*" (IT.2)<br>- "*[The IT department] now takes into account the service providers as without them, [they] cannot have services. So [they] try to keep a professional transparent relationship with them*" (IT.7) |

Figure 27 represents the different relational mechanisms that emerged from our interviews, adopted along with cloud services.

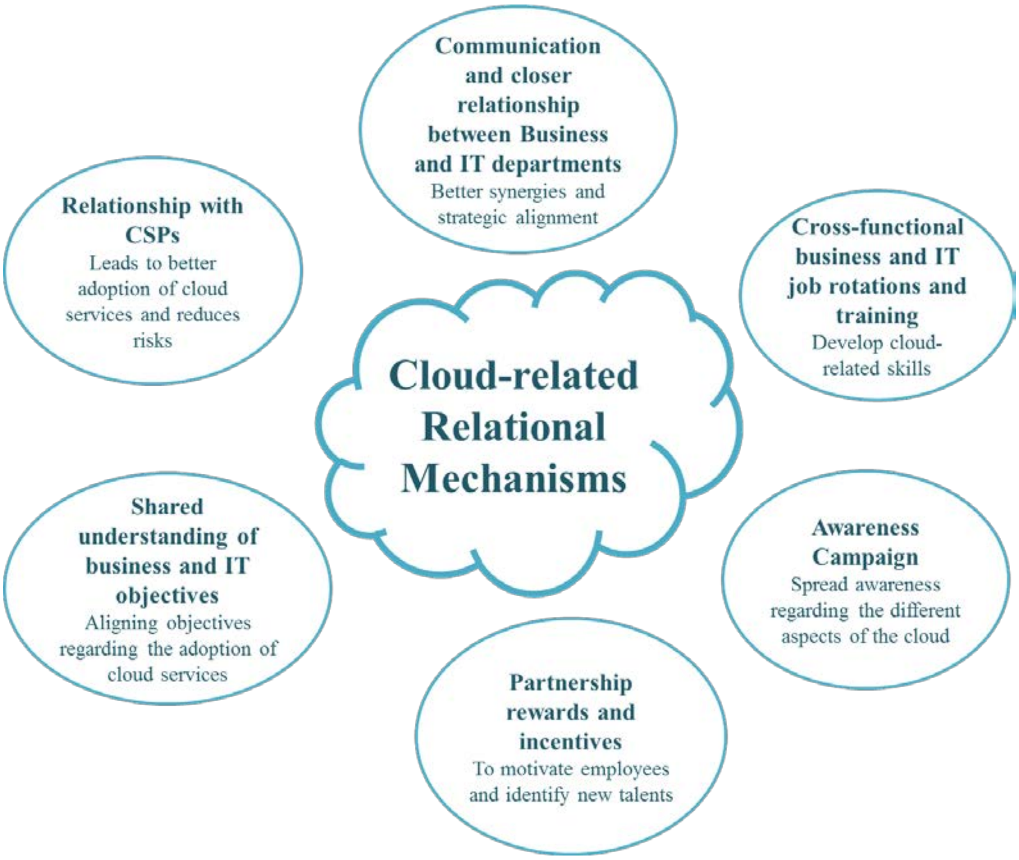


**Figure 27: Emerged relational mechanisms for cloud services**

## VI. Cloud Contracts

As the regulatory part plays an essential role in cloud solutions adoption, agreeing on CSPs' contracts is a vital step. As data analysis highlights the importance of contracts, particularly three clauses (reversibility, confidentiality, and SLAs clauses), it also shows the steps organizations take before signing a contract.

Cloud contracts are extremely important for several issues. The most important clause for most organizations is the reversibility one (IT.2, IT.3, IT.5, IT.6, IT.9, IT.10, IT.11, IT.12, IT.13, IT.15, B.8, IT.16, IT.17, IT.20, IT.19, B.10, IT.23). Before signing any cloud contract, "*[they] immediately flip to the reversibility clause to check the terms*" (IT.15). It seems reassuring for organizations when the CSP provides them with data that are written in a universal programming language, and can be used on different platforms. However, when the CSP codes the data in their own specific language, it becomes difficult for the organization to export them and use them elsewhere; their data will be useless and they will have to start from zero. In this respect, some organizations (IT.15, IT.13, IT.5) try to negotiate with their CSPs and impose programming languages that work for them. Nevertheless, this clause is not always negotiable, particularly when CSPs offer their clients standardized contracts. Therefore, the reversibility clause needs to be cautiously read and agreed upon by the organization.

In addition, the confidentiality clauses need to be well written and agreed upon. Organizations need to make sure of the presence of "*data protection and data location in the European countries*" (IT.9, IT.11, IT.12, B.4, IT.15, IT.16, IT.19, IT.20, B.10, IT.23). They require a guarantee that their confidential data will not be accessed or used by third parties without their consent. In fact, due to the issuance of many laws, organizations do not feel safe storing their data outside the European zone. Therefore, the confidentiality clause is also another clause that needs to be read meticulously.

Additionally, data findings highlight the importance of the reliability of cloud services and their promised quality. Before choosing the CSP, "*[they] check their proposed SLA, which plays an important part in [their] decisions*" (B.5), especially since "*[they] do not wish to have an outage when dealing with important deadlines*" (B.7). When organizations sign a contract according to an agreed SLA, they are assured that the adopted cloud solutions will be reliable up to the agreed SLA.

Moreover, data analysis portrayed the way organizations handle contracts. Negotiating a contract appears to be a long process as "*it takes 18 months to negotiate a large contract related to IaaS or PaaS solutions*" (IT.8). Therefore, organizations that need to negotiate contracts with their CSPs usually sign them for a "*5-year period*" (IT.12). However, SaaS solutions are usually lighter. They are bought through monthly or yearly subscriptions, where most CSPs offer their clients a "*10-20% discount if they subscribe yearly instead of monthly*" (IT.14). This presents an economic advantage since "*if the monthly price would increase, [they] will not get affected*" (IT.24). Similarly, CSPs prefer this method where they have guarantees that throughout the year, clients will not switch to another CSP (IT.24).

# Part II: Phase II of Interviews

Our first round of interviews highlights the need of taking the right decisions when adopting cloud technologies. It also identifies the mechanisms organizations seem to deploy in order to govern their cloud services and benefit from their advantages. New structures and relational mechanisms were "instinctively" implemented within organizations. While some of the implemented mechanisms emanate from existing IT governance models such as ITIL, COBIT or CMMI frameworks, some mechanisms come from agile or other management approaches (such as scrum methodology).

Thus, organizations do not seem to have a specific framework for governing cloud services even though data highlight the need of cloud governance. Regarding the transformations that cloud computing induces in organizations, IT governance frameworks are not enough solely. Governance mechanisms that are cloud oriented are therefore necessary. In this respect, it appears to be useful to evaluate the maturity level of the cloud service adoption.

For this purpose, we conducted a second round of interviews with the same sample of organizations. These interviews were based on a number of close-ended questions. These questions emanate from one of the rare cloud governance framework we identified in the professional literature (ODCA, 2013). The aim of this second round of interviews was to asses which governance mechanisms where deployed within organizations and the maturity level of cloud adoption in these organizations. This second round of collecting data aims at identifying the relationship between cloud governance and the intensity level of adopting cloud computing.

## I. Group Classification

This section discusses the analysis results of the second round of interviews with the 35 participants. It is important to note that we are interested in calculating the maturity level of the cloud services adoption in the 35 organizations. Accordingly, we will base our assessment work on the Cloud Maturity Model (CMM) offered by the ODCA (2013).

By drawing on ODCA (2013), we identified 18 questions that cover 8 domains related to cloud maturity adoption: business strategy; organization and skills; governance; projects, portfolio and services; architecture; operations; infrastructure; information. The questions can be found in the Appendix II. Each question has five possible responses (Cloud Maturity Evaluation). The level 1 (CMM1) is linked to an "ad hoc use of cloud services" and level 5 (CMM5) to an "optimal adoption of cloud services". By answering each one of the 18 questions, the respondent will get a number assessing the maturity level associated with his answer. If during a question, participants felt hesitant regarding the level in which their organization belongs, the average level of the two was taken into account. This explains the presence of decimals in Table 26. For example, regarding Q1 participant IT.7 hesitated between "*Yes, but with ad-hoc adoption*" and "*Well communicated throughout the organization and signed off by all key stakeholders*". He explained that their cloud strategy is more than Ad Hoc implemented, but it is still not well communicated throughout the whole organization. With this answer, and under the agreement of the participant, we decided to allocate a level of 2.5 for this question.

The section below reviews the questions that have been addressed during the interview as well as the results. Table 26 presents the score of each organization based on the answer they gave to each question. This score sheds light on the maturity level of each domain and the remaining efforts that organizations should deploy in each domain in order to increase their maturity level in cloud adoption. This maturity level is fundamental for effectively governing the cloud and benefit from the associated advantages.

**Table 26: Results of second round of interviews (cf. Appendix II for questions)**

| | Strategy | | | Organization and Skills | | | Governance | | | | Projects, Portfolio and Services | | Architecture | Operations | Infrastructure | | | Information |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Q1** | **Q2** | **Q3** | **Q4** | **Q5** | **Q6** | **Q7** | **Q8** | **Q9** | **Q10** | **Q11** | **Q12** | **Q13** | **Q14** | **Q15** | **Q16** | **Q17** | **Q18** |
| **IT.16** | 2 | 3 | 2 | 4 | 3 | 3 | 3 | 4 | 3 | 3 | 2 | 3 | 3 | 3 | 2 | NA | 4 | 3 |
| **IT.7** | 2,5 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 2,5 | 2,5 | 2,5 | 2,5 | 2,5 | 3 | 3 | NA | 4 | 3 |
| **IT.24** | 2,5 | 3 | 3 | 3 | 2,5 | 2 | 2,5 | 2 | 3 | 2,5 | 2,5 | 2,5 | 3 | 3 | 2,5 | 3 | 4 | 3 |
| **IT.5** | 2,5 | 2,5 | 2 | 2,5 | 3 | 2 | 2,5 | 2 | 3 | 2 | 2 | 2 | 3 | 2 | 2 | NA | 4 | 3 |
| **IT.8** | 2 | 2,5 | 2 | 2,5 | 3 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 3 | 2 | 2 | NA | 3 | 2 |
| **IT.12** | 2 | 2 | 1 | 2 | 3 | 3 | 2 | 2,5 | 2 | 2 | 1 | 2 | 3 | 2,5 | 1,5 | NA | 4 | 2 |
| **IT.3** | 1 | 2 | 1 | 2 | 1 | 1 | 1 | 3 | 2 | 1 | 1 | 1 | 3 | 3 | 3 | 4 | 4 | 3 |
| **B.9** | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | NA | 4 | 3 |
| **IT.14** | 2 | 2 | 1 | 2 | 2 | 1,5 | 1 | 2 | 2 | 3 | 1 | 1,5 | 3 | 2 | 2 | NA | 4 | 2,5 |
| **IT.11** | 2 | 2 | 1 | 2 | 1,5 | 1,5 | 1 | 2 | 2 | 3 | 1 | 1,5 | 3 | 2 | 2 | NA | 4 | 2,5 |
| **IT.18** | 2 | 2,5 | 2 | 2 | 2,5 | 2 | 1,5 | 2 | 1,5 | 2 | 2 | 2 | 2,5 | 1,5 | 2 | NA | 4 | 2 |
| **IT.22** | 3 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 3 | 2 | 1 | 2 | 2 | 2 | 2 | NA | 3 | 2 |
| **B.11** | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 1 | 2 | 2 | 2 | 2,5 | NA | 3 | 2 |
| **IT.15** | 2,5 | 2 | 2 | 2,5 | 2 | 1,5 | 1,5 | 2 | 2 | 2 | 2 | 1,5 | 2 | 2 | 2 | NA | 4 | 2 |
| **IT.2** | 3 | 1 | 1 | 1 | 1 | 2 | 3 | 4 | 2 | 2 | 3 | 2 | 2 | 1 | 1 | 3 | 4 | 3 |
| **B.6** | 2 | 3 | 1 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | NA | 3 | 2 |
| **B.10** | 2,5 | 2 | 1,5 | 2 | 1,5 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 1,5 | 2 | NA | 4 | 2 |
| **IT.4** | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 1 | 2 | 1 | 2 | 2 | 2 | 2 | NA | 3 | 2 |
| **B.4** | 2 | 1,5 | 2 | 1,5 | 2 | 1,5 | 1 | 2 | 1,5 | 1,5 | 1 | 1,5 | 2 | 2 | 1 | NA | 4 | 2 |
| **IT.23** | 1 | 1,5 | 1,5 | 2 | 2 | 1,5 | 1,5 | 2 | 2 | 1,5 | 1,5 | 1,5 | 2 | 1,5 | 1,5 | 3 | 4 | 2 |
| **IT.21** | 2 | 2 | 1 | 2 | 2 | 2 | 1 | 2 | 1 | 2 | 2 | 1 | 1,5 | 1 | 2 | NA | 4 | 2 |
| **IT.13** | 2 | 1,5 | 1,5 | 1,5 | 2 | 2 | 2 | 2 | 2 | 1,5 | 1,5 | 1,5 | 1,5 | 1 | 1,5 | 3 | 4 | 2 |

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **B.8** | 2 | 2 | 2 | 1,5 | 1,5 | 1,5 | 1,5 | 2 | 2 | 2 | 1,5 | 1,5 | 1,5 | 1 | 2 | 3 | 4 | 1,5 |
| **IT.6** | 1,5 | 1,5 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 1 | 1,5 | 2 | 1,5 | 2 | 4 | 1,5 |
| **IT.17** | 2 | 1 | 2 | 1 | 1 | 1 | 1,5 | 3 | 1 | 2 | 0,5 | 1 | 2 | 1 | 2 | NA | 4 | 2 |
| **IT.9** | 1,5 | 1 | 0 | 2 | 1 | 1 | 1 | 2 | 1 | 1 | 0,5 | 2 | 2 | 1 | 1 | NA | 4 | 3 |
| **IT.10** | 2 | 1 | 0 | 2 | 1,5 | 1 | 1 | 2 | 1 | 1 | 0 | 2 | 2 | 1 | 1 | 2 | 4 | 3 |
| **IT.20** | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1,5 | 1 | 1 | 1 | 1 | 2 | 2 | NA | 4 | 2 |
| **B.5** | 2 | 2,5 | 2 | 2 | 1 | 1,5 | 1 | 2 | 1,5 | 1 | 1 | 1 | 1 | 1 | 1,5 | NA | 4 | 1,5 |
| **IT.19** | 1 | 1 | 1 | 1,5 | 1 | 1 | 1 | 2 | 1,5 | 1 | 1 | 1 | 1 | 1 | 2 | NA | 4 | 2 |
| **IT.1** | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 2 | 1 | 1 | 0,5 | 1 | 1 | 0,5 | NA | 3 | 3 | 1 |
| **B.1** | 1 | 2 | 2 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 2 | 1 | 1 | NA | NA | 1 | 1 |
| **B.2** | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 0,5 | 1 | 1 | 0,5 | NA | NA | 2 | 2 |
| **B.7** | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | NA | NA | 1 | 1 |
| **B.3** | 1 | 0,5 | 0,5 | 0,5 | 1 | 1 | 0,5 | 1 | 1 | 1 | 1 | 1 | 0,5 | 0,5 | 1 | NA | 3 | 1 |

After collecting the answers related to the 18 questions, we first calculated the average of each domain (8 domains), which are represented in Table 27. This average gave us an idea of the maturity level per domain for each organization.

For example, according to the answers provided by IT.16, their organization has a **Strategy** maturity of 2.333 over 5 and a **Governance** of 3.25. This score implies that the strategy maturity level is located in the CMM2 level, while its **Governance** is located in the CMM3 level according to ODCA (2013). Thus, if we view this score according to the Table 10 (cf. Cloud Maturity Evaluation), having a CMM2 level **Strategy** implies having departmental cloud strategies applied along with opportunistic leverage of cloud services. In addition, having a CMM3 level **Governance** signifies that a cloud governance is integrated within its organizational governance practices. In fact, Table 27 along with Tables 10, 11 and 12 (cf. Cloud Maturity Evaluation) helped us assess the maturity of each organization according to the 8 domains presented by the ODCA (2013).

In order to better illustrate the way organizations can assess themselves by drawing on the relationship between the cloud maturity tables found in the literature (Tables 10, and 11) and their actual score, we will present the score of IT.3 (for random reasons). According to IT.3

their organization has an **Infrastructure** maturity of 3.5 while its **Project, Portfolio and Services** maturity is 1. This leads to the conclusion that the organization of IT.3 is mature regarding its cloud **infrastructure**, but still immature in its cloud **projects**. Thus, in this organization, cloud projects and changes occur with Ad Hoc controls and designs, where cloud projects lifecycles do not intersect. However, they have a private PaaS framework where transition and transformation processes occur with cloud solutions. This example illustrates a gap between two domains, where one is mature enough and the other needs improvement. The organization, thus, knows that it should enhance and improve its cloud **projects** domain. Therefore, based on the average results, organizations can enhance the domains that they think possess a low cloud maturity level. As each domain is increasing in maturity, the overall cloud maturity is increasing as well. The ODCA (2016) affirms that moving from one maturity level to the other takes on average 12 months.

**Table 27: Domains average maturity**

| | Strategy | Organization and Skills | Governance | Projects, Portfolio and Services | Architecture | Operations | Infrastructure | Information |
|---|---|---|---|---|---|---|---|---|
| **IT.16** | 2,333 | 3,333 | 3,25 | 2,5 | 3 | 3 | 3 | 3 |
| **IT.7** | 2,833 | 3 | 2,75 | 2,5 | 2,5 | 3 | 3,5 | 3 |
| **IT.24** | 2,833 | 2,5 | 2,5 | 2,5 | 3 | 3 | 3,167 | 3 |
| **IT.5** | 2,333 | 2,5 | 2,375 | 2 | 3 | 2 | 3 | 3 |
| **IT.8** | 2,167 | 2,5 | 2,25 | 2 | 3 | 2 | 2,5 | 2 |
| **IT.12** | 1,667 | 2,667 | 2,125 | 1,5 | 3 | 2,5 | 2,75 | 2 |
| **IT.3** | 1,333 | 1,333 | 1,75 | 1 | 3 | 3 | 3,5 | 3 |
| **B.9** | 2 | 2 | 2,25 | 1,5 | 2 | 2 | 3 | 3 |
| **IT.14** | 1,667 | 1,833 | 2 | 1,25 | 3 | 2 | 3 | 2,5 |
| **IT.11** | 1,667 | 1,667 | 2 | 1,25 | 3 | 2 | 3 | 2,5 |
| **IT.18** | 2,167 | 2,167 | 1,75 | 2 | 2,5 | 1,5 | 3 | 2 |
| **IT.22** | 2,333 | 2,333 | 2,25 | 1,5 | 2 | 2 | 2,5 | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **B.11** | 2 | 2,333 | 2,25 | 1,5 | 2 | 2 | 2,75 | 2 |
| **IT.15** | 2,167 | 2 | 1,875 | 1,75 | 2 | 2 | 3 | 2 |
| **IT.2** | 1,667 | 1,333 | 2,75 | 2,5 | 2 | 1 | 2,5 | 3 |
| **B.6** | 2 | 2,333 | 2 | 1,5 | 2 | 2 | 2,5 | 2 |
| **B.10** | 2 | 1,833 | 2 | 1,5 | 2 | 1,5 | 3 | 2 |
| **IT.4** | 2 | 1,667 | 1,75 | 1,5 | 2 | 2 | 2,5 | 2 |
| **B.4** | 1,833 | 1,667 | 1,5 | 1,25 | 2 | 2 | 2,5 | 2 |
| **IT.23** | 1,333 | 1,833 | 1,75 | 1,5 | 2 | 1,5 | 2,667 | 2 |
| **IT.21** | 1,667 | 2 | 1,5 | 1,5 | 1,5 | 1 | 3 | 2 |
| **IT.13** | 1,667 | 1,833 | 1,875 | 1,5 | 1,5 | 1 | 2,667 | 2 |
| **B.8** | 2 | 1,5 | 1,875 | 1,5 | 1,5 | 1 | 2,833 | 1,5 |
| **IT.6** | 1,333 | 2 | 2 | 1 | 1,5 | 2 | 2,333 | 1,5 |
| **IT.17** | 1,667 | 1 | 1,875 | 0,75 | 2 | 1 | 3 | 2 |
| **IT.9** | 0,833 | 1,333 | 1,25 | 1,25 | 2 | 1 | 2,5 | 3 |
| **IT.10** | 1 | 1,5 | 1,25 | 1 | 2 | 1 | 2,333 | 3 |
| **IT.20** | 1 | 1 | 1,375 | 1 | 1 | 2 | 3 | 2 |
| **B.5** | 2,167 | 1,5 | 1,375 | 1 | 1 | 1 | 2,75 | 1,5 |
| **IT.19** | 1 | 1,167 | 1,375 | 1 | 1 | 1 | 3 | 2 |
| **IT.1** | 1 | 1,333 | 1,25 | 0,75 | 1 | 0,5 | 3 | 1 |
| **B.1** | 1,667 | 1 | 1,25 | 1,5 | 1 | 1 | 1 | 1 |
| **B.2** | 0,667 | 1 | 1,25 | 0,75 | 1 | 0,5 | 2 | 2 |
| **B.7** | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| **B.3** | 0,667 | 0,833 | 0,875 | 1 | 0,5 | 0,5 | 2 | 1 |

## II. Group Analysis

Table 28 represents the total maturity average of the 35 organizations (in descending order). The organization of IT.16 is the most mature one with a total maturity average of 2.927. According to ODCA (2016), the level of maturity of this organization is CMM3.

Our 35 large French organizations were classified into three groups according to their Total Maturity Average. These groups were divided this way based on their rounded maturity average to the nearest number (1.0, 2.0 or 3.0). Based on the questions answered, we will analyze the classification of the organizations into these three groups. According to ODCA (2016), CMM3 represents a systematic maturity level, where the various parties have approved of the proposed approach in CMM2, in addition to an importance allocated to governance and risk tools in the control layer. Moreover, the CMM3 level implies the emergence of private PaaS with a sophisticated adoption of SaaS solutions.

**Table 28: Total maturity average**

| Participants | Total Maturity Average | Cloud Maturity Level |
|---|---|---|
| **Group 1** | | |
| **IT.16** | 2,927 | CMM3 |
| **IT.7** | 2,885 | |
| **IT.24** | 2,813 | |
| **IT.5** | 2,526 | |
| **Group 2** | | |
| **IT.8** | 2,302 | CMM2 |
| **IT.12** | 2,276 | |
| **IT.3** | 2,240 | |
| **B.9** | 2,219 | |
| **IT.14** | 2,156 | |
| **IT.11** | 2,135 | |
| **IT.18** | 2,134 | |
| **IT.22** | 2,115 | |

| | | |
|---|---|---|
| **B.11** | 2,104 | |
| **IT.15** | 2,099 | |
| **IT.2** | 2,094 | |
| **B.6** | 2,042 | |
| **B.10** | 1,979 | |
| **IT.4** | 1,927 | |
| **B.4** | 1,844 | |
| **IT.23** | 1,823 | |
| **IT.21** | 1,771 | |
| **IT.13** | 1,755 | |
| **B.8** | 1,714 | |
| **IT.6** | 1,708 | |
| **IT.17** | 1,661 | |
| **IT.9** | 1,646 | |
| **IT.10** | 1,635 | |
| **IT.20** | 1,547 | |
| **B.5** | 1,536 | |
| **Group 3** | | |
| **IT.19** | 1,443 | CMM1 |
| **IT.1** | 1,229 | |
| **B.1** | 1,177 | |
| **B.2** | 1,146 | |
| **B.7** | 1,000 | |
| **B.3** | 0,922 | |

**Group 1** encompasses organizations with the highest total maturity average belonging to the CMM3 level. Thus, these organizations possess the highest intensity level of their adoption of cloud services. They are on the right path to immerse themselves in cloud solutions.

According to Q8 and Q18 (cf. Appendix II), the organizations stated that their risk management as well as their security skills are updated for cloud solutions. These organizations fully understand that CC does not come free of risks. Thus, while their security risks are high, they work on finding ways to mitigate them. This is a proof of adopting a high amount of cloud services, as organizations do not feel inhibited by the different risks generated by these solutions; instead, they are developing their capabilities and learning how to face them. In addition, these organizations offer formal cloud trainings for their employees in order to teach them how to deal with the adopted cloud solutions (Q5). They are aware that dealing with cloud services is different from services implemented on-premises, where employees need updated skills and new competences. Moreover, IT.16, IT.7, IT.24 and IT.5 discovered the importance of compliance when dealing with sensitive data stored on public clouds. This pushed them to put a lot of focus on implementing a formal compliance framework for CC (Q9). Concerning the governance mechanisms, it seems that the structures and processes are highly important for these participants, as answered in Q4, Q13, and Q14. This proves that these organizations want to increase their cloud adoption, as they understood that in order to govern cloud solutions, governance mechanisms need to be implemented to work together and guide them through the desired organizational behaviors. Finally, as positive characteristics, these organizations have formulated an enterprise strategy positioning the use of cloud solutions (Q1) and have implemented a cloud adoption framework (Q2).

**Group 1** has shown several signs of high adoption according to the preceding questions. However, the four organizations still need to work on a few issues, in order to reach an optimal adoption. For example, it appears that they need to fortify the role of their internal IT (Q6). In addition, increasing their communication plans (Q7) would make the organization more aware of cloud solutions needs and hence, increase their adoption. Such relational mechanisms are relatively easy to implement while their impact is grand. Moreover, Key Performance Indicators (KPIs) play an important role in the organization’s strategy as they measure the progress of the organization towards achieving their desired strategy and goal. These organizations are advised to develop further their KPIs (Q3) and apply them in measuring the performance generated by cloud solutions. Finally, these organizations marked their infrastructure and platform as not too developed (Q15 and Q16), where only one organization has implemented a PaaS solution so far. Thus, they are also advised to work on these issues as well. Even if the questions address a variety of subjects (strategy, operations, performance, etc.), our aim is to focus on the average results in order to assess the intensity level of adoption of cloud services for each organization.

**Group 2** includes the highest number of organizations (IT.8, IT.12, IT.3, B.9, IT.14, IT.11, IT.18, IT.22, B.11, IT.15, IT.2, B.6, B.10, IT.4, B.4, IT.23, IT.21, IT.13, B.8, IT.6, IT.17, IT.9, IT.10, IT.20, and B.5). They are classified in the CMM2 level, meaning their cloud maturity is opportunistic; they are aware of the benefits generated by cloud solutions, but are still wary about the risks. This is what inhibits them from increasing their cloud adoption. Similar to Group 1, according to Q8 and Q18, risk management and security skills are well ranked for most organizations, leading to the conclusion that the risks generated by CC are taken into consideration. While most organizations are working on their architecture processes (Q13), only some are updating their structures to enable cloud solutions delivery (Q4). This shows that most of these organizations that want to become more mature are aware of the importance of governance mechanisms. However, they still have a long way to go in order to adopt optimally cloud services (CMM5). Additionally, some organizations are working on updating their enterprise strategy for CC (Q1). Finally, although organizations are working on their cloud infrastructures (Q15), they are advised to improve it and develop the capabilities related to it, as well as develop their PaaS adoption (Q16).

Nevertheless, being in a CMM2 level signifies that organizations still need to transition in several areas and develop numerous cloud capabilities in order to optimally adopt cloud services. Table 27 highlights many areas in which organizations are advised to develop. For instance, they should start by implementing a communication plan (Q7) in order to raise awareness regarding cloud solutions, in addition to offering cloud trainings (Q5) and developing project skills (Q12). Through this communication plan, employees will be more aware of the demands of CC, which will push them to attend training sessions (that should be offered by the organization) and thus increasing their cloud skills. Additionally, project tools are not updated for CC (Q11) while processes are not generally adopted (Q14). Meanwhile, the role of internal IT does not support cloud adoption (Q6). Therefore, organizations should focus on the role that the internal IT plays in the cloud adoption process, in order to strengthen the links between the different departments. Finally, a primordial issue related to cloud computing is the contracts. These organizations, however, do not pay much attention to cloud contracts (Q10). This is a merciless mistake as organizations are safe and are linked to CSPs through these contracts.

**Group 3** includes six organizations with a very low cloud adoption. They possess a preliminary view of cloud solutions where they only use them for basic or special needs. While they focus more on the risks generated by CC, they are controlled by the security and compliance risks, which inhibit them from adopting more sophisticated cloud solutions. This is illustrated by Q8, Q9, and Q18 (cf. Appendix II), where organizations possess a relative-high level regarding their risk management, while trying to be compliant and develop their security skills.

Nonetheless, these organizations have an extremely shallow vision of CC. They have to work on several aspects. For instance, these organizations do not possess a cloud adoption framework (Q2) or a formal enterprise strategy for cloud solutions (Q1), which represent the foundation of CC. Additionally, they do not implement governance processes adapted for CC (Q14), or architecture processes (Q13) for the basis of CC. Moreover, their project tools are not implemented (Q11), where their project skills (Q12) and communication plans (Q7) are not developed. Finally, while cloud contracts are disregarded by these organizations (Q10), KPIs are not implemented (Q3). This explains their low cloud maturity levels, where they simply do not adopt sophisticated cloud solutions.

## III. Cloud Maturity Model Levels Verification

Along with this analysis, we decided to compare the Cloud Maturity Model levels proposed by the ODCA (2016) with the three groups, to determine whether our conclusions are pertinent. Starting with Group 1, where we stated that they possess a CMM3 level. The ODCA (2016) defined this level as a "*the proposed approach in CMM2 has been finally reviewed and accepted by the various parties. The important part of this level is the introduction of governance and risk tools in the control layer, which pushes the organization to follow the corporate requirements and regulations. In addition, organizations observe an emergence of a private PaaS with a sophisticated implementation of SaaS solutions*". From our analysis, we can clearly state that the organizations of Group 1 did introduce *governance and risk tools*, which helped them reach this level of maturity. In addition, one organization implemented *PaaS* solutions.

The CMM2, associated to Group 2, is defined by the ODCA (2016) as "I*n this level, organizations fully embraced their private cloud while thinking of moving some applications to the cloud. For instance, cloud-aware applications are being part of the board's* *discussions. While an approach has been applied opportunistically, it has not been widely accepted yet*". Organizations of the Group 2 have all *embraced their private clouds*. Based on the mechanisms adopted by these organizations, we can say that *the CC approach has not been widely accepted yet*.

Finally, the CMM1, representing the maturity level of Group 3, is defined, "*While the organization still possesses its physical infrastructure, some virtualized systems exist already. However, they are operated under traditional IT processes and lack automation. Some cloud computing awareness is spread throughout the organization, while some teams are starting to adopt few cloud solutions. In addition, organizations feel safer at this stage to implement their private cloud, while adopting some basic public SaaS solutions.*" (ODCA, 2016, cf. Cloud Maturity Evaluation). Organizations of Group 3 *are operated under their traditional IT processes and lack automation, where some teams are adopting few basic SaaS cloud solutions*.

After this in-depth analysis of the three groups, it appears that most organizations address the CC subject from a risk perspective as their risk management and security skills are highly develop. They are all aware of the risks generated by CC, which plays a role in inhibiting them from going further in the cloud world. In addition, the lack of skills and competences also plays a role in the cloud maturity level, where employees are oblivious about the ways to adopt cloud solutions. Hence, while some organizations (Group 1) have developed cloud capabilities, facilitating their adoption of cloud services, others are following them but at a slower pace.

# IV. Spider Charts Illustrations

Spider charts are another representation to show organizations which domains need development. Figure 28 and Figure 29 illustrate the spider charts of two organizations belonging to Group 1 (CMM3). While all domains need improvement in order to reach a cloud maturity level of 5, the organization of IT.16 mostly needs to improve their **Strategy** and **Projects** domains where they have values close to 2 (Figure 28). They can work on adapting their strategy on cloud services as well as develop more cloud-related projects. The organization of IT.5 possesses domains with very close maturity, their **Operations,** their **Strategy**, their **Organization and Skills**, their **Governance**, and their **Projects** have a value close to 2 (Figure 29). These two figures (Figure 28 and Figure 29) prove that the organizations' domains are balanced, where they are developing all domains quasi-equally, which is another sign of a higher adoption intensity level.

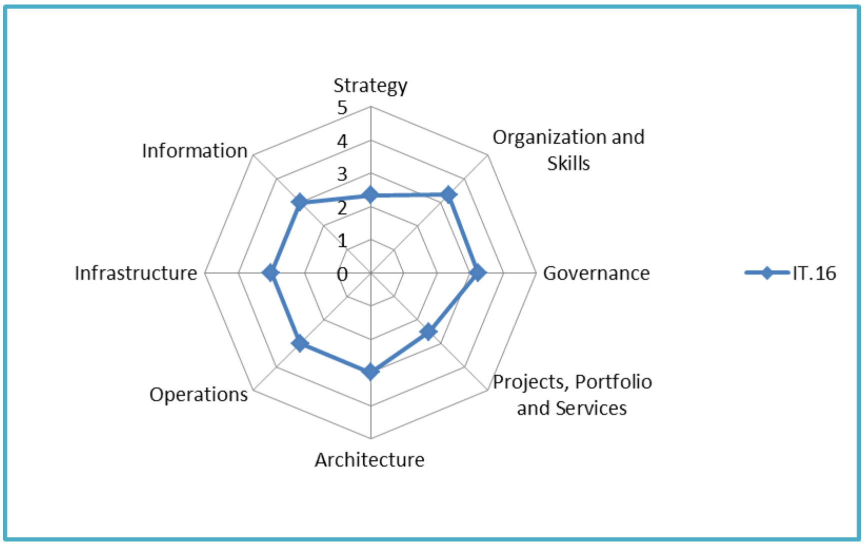


**Figure 28: Domains average maturity for IT.16**

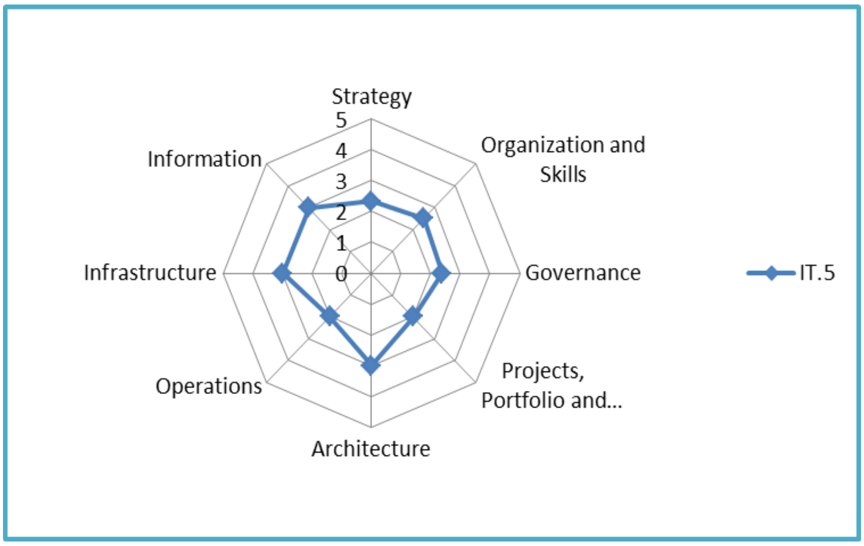


**Figure 29: Domains average maturity for IT.5**

Figure 30 and Figure 31 illustrate the organizations of IT.2 and IT.10, from the Group 2 (CMM2). The spider chart of IT.2 shows that the organization has some domains more developed than others, such as the **Information**, **Infrastructure**, **Governance**, and **Projects**. However, the **Operations**, **Organization and Skills**, and **Strategy** domains need more effort and development in order to reach a higher cloud maturity level. Through this chart, the organization can know where to focus its attention. Moreover, the spider chart of IT.10 looks completely unbalanced, which should be alarming for the organization. They clearly need to develop all of their domains, specifically their **Operations**, **Strategy**, **Organizations and**

**Skills**, **Governance** and **Projects** domains. These two spider charts also emphasize the low cloud adoption level of organizations, where focus is not equally distributed among all domains.

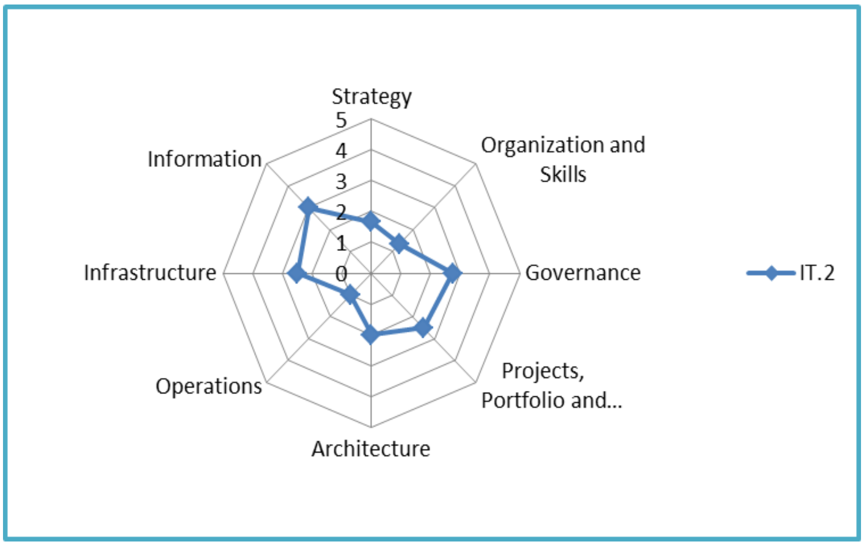


**Figure 30: Domains average maturity for IT.2**

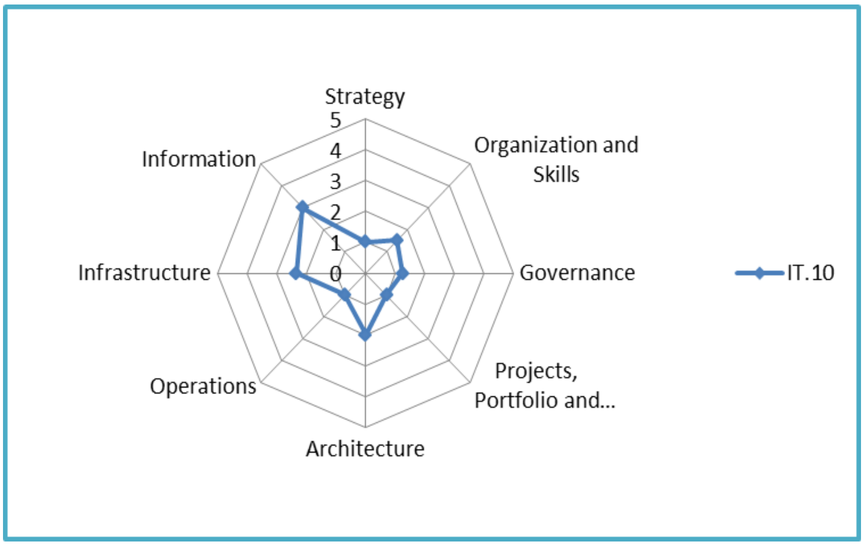


**Figure 31: Domains average maturity for IT.10**

Furthermore, Figure 32 and Figure 33 illustrate the spider charts of the last Group for two organizations (IT.1 and B.3). These charts prove that these organizations have a preliminary adoption of cloud solutions, where all of the domains need critical focus and hence, serious development. They both have their **Infrastructure** domain more developed than others, which is logical given that these organizations installed either a private IaaS or a private PaaS.

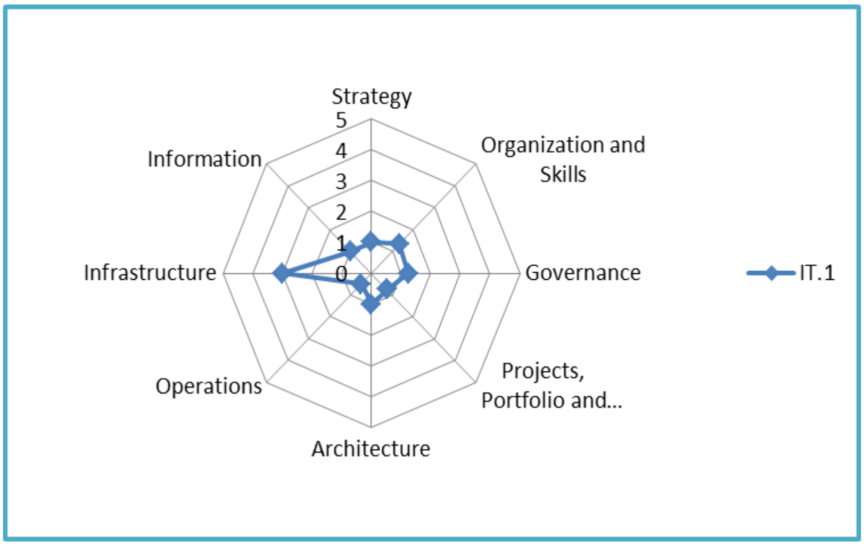


**Figure 32: Domains average maturity for IT.1**

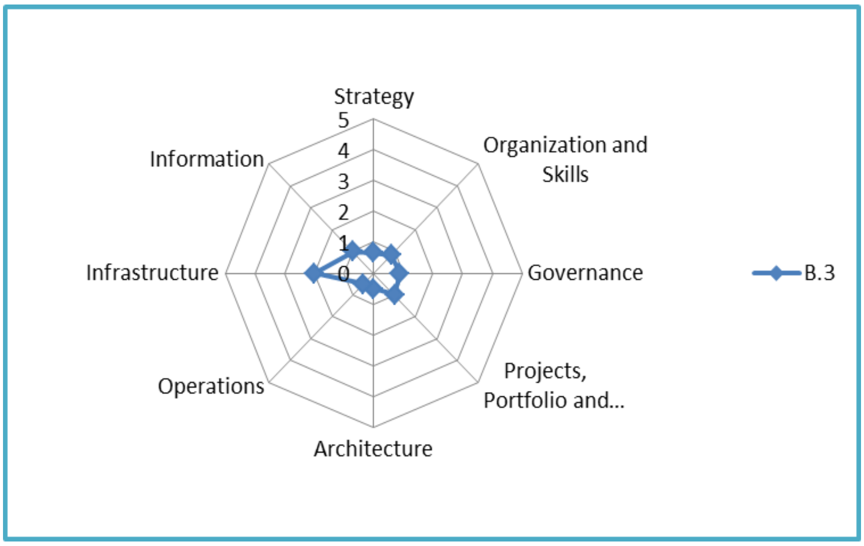


**Figure 33: Domains average maturity for B.3**

Figure 34 regroups the spider charts of the 6 participants shown above. It emphasizes the apparent difference between the various groups. While some organizations have the highest maturity in **Organization and Skills** (IT.16 and IT.5) for example, others possess their lowest maturity in **Operations** (IT.1 and B.3). It is important to visualize the way organizations evolve in the different domains when adopting cloud services.

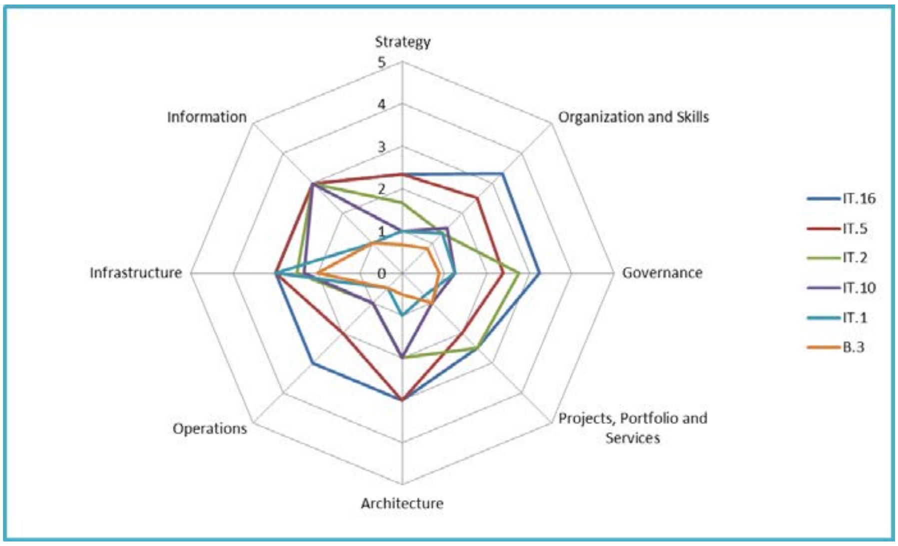


**Figure 34: Spider chart of the 6 previous examples**

## V. In-depth Analysis

In order to deepen our analysis even more, it would be interesting to explore the mechanisms adopted by these three groups, their decision making processes, the decisions discussed, their education level, and the corporate strategies pushing them to adopting CC.

Table 29 illustrates the various factors influencing the intensity level of cloud adoption in the 35 organizations. They are presented in a descending order, from the organization that has the highest cloud maturity score (IT.16 – 2.927) to the one with the lowest cloud maturity score (B.3 – 0.922). From these factors, Table 29 shows the importance of IT governance (the various cloud-related governance mechanisms, the locus of decisions, the decision makers, and the cloud-decisions addressed), the influence of the education of employees (level of skills, the syndicates, and the education system), and the role of the corporate strategy behind the adoption of cloud services.

As shown in Table 29, organizations of **Group 1**, possessing a maturity level of CMM3, share several characteristics. First, they have implemented so far several governance mechanisms through different structures, processes, or even relational ones that work together to help them govern cloud decisions. While IT governance is affected by the implementation of mechanisms, cloud maturity level of each organization will depend on the adoption level of governance mechanisms. In addition, these organizations share their locus of decisions, which is decentralized, where the decision making process happens through a collaboration between the different departments. The collaboration is a sign of a mature organization, where all departments possess a voice and are able to express it. Nevertheless, when needed, the IT department arbitrates the final decision for some organizations. Furthermore, in order to fully assess the IT governance of these organizations, we had to check the different decisions they discuss. For instance, during their meetings, organizations of Group 1 discuss various advanced decisions such as the economic benefits of adopting cloud services, its security threats, the need of new skills, the cloud contracts, the technical transitions, etc. These decisions show an advanced level of adoption. Therefore, based on the cloud-related mechanisms, the decision-making process, and the decisions discussed, cloud services are well governed for these organizations, leading to a higher cloud intensity level of adoption.

In order to assess the education level of each organization, it emerges from the analysis that it is divided into three subcategories: level of developed skills, education of syndicates, and the education system. The level of their developed skills is assessed via the questionnaire (Q4, Q5, and Q6). As illustrated in Table 29, Group 1 possesses an **Organization and Skill** level of almost 3, meaning that their skills are moving from being operational to strategic, providing the organization with a better competitive advantage. In addition, based on the relational mechanisms cited by participants from Group 1, they have implemented cross-functional trainings, pushing employees on developing their skills and increase their knowledge in cloud computing. Furthermore, some participants agreed that "*training employees is a must*" (IT.16) while discussing it during the decision making process, "*How many training sessions should we have per month to stay updated*" (IT.7). Since we interviewed French organizations, with a high rate of employees who received their degrees in France, the education system is a common factor to the 35 organizations. This means that an organization based in a country having a more adapted education system to the digital transformation is prone to have a higher cloud maturity. Regarding the education of syndicates, it can be considered a common factor for all organizations as well. The main syndicates for employees in France are the following: "Confédération française de l'encadrement - Confédération générale des cadres" (CFE-CGC), "Confédération française démocratique du travail" (CFDT), "Confédération française des travailleurs chrétiens" (CFTC), "Confédération générale du travail" (CGT), "Confédération générale du travail - Force ouvrière" (CGT-FO). Finally, these organizations share the same motivation for adopting cloud services. Their motivation is to stay in the competition loop. These organizations focus on competition and do not want to be beaten by other organizations from the same industry. For example, IT.7 is the CIO of a Media and Entertainment organization, where competition plays an extremely serious issue. IT.7 mentioned that with the emergence of CC, new organizations are building up, especially in the media industry, where "*they're stealing some of [their] market shares*". He elaborated that these startups are tough competitors, as "*they do not own the legacy to slow them down*". Therefore, they are a huge threat to large organizations, which cannot detach from their legacy history. All of this pushes such organizations to be competitive, and hence have a high cloud maturity, in order to stay in the market. Therefore, this emphasizes the importance of the adoption level of mechanisms, the corporate strategies of CC adoption, the locus of decisions, and the decision makers' role in the cloud maturity level of the organization.

**Group 2** possesses the largest number of organizations (25), whose cloud maturities range between 1,536 (B.5) and 2.302 (IT.8) as represented in Table 29. It is interesting to notice how close their cloud maturities are. One can notice that their cloud maturity is proportionally decreasing to the number of mechanisms implemented in the organizations. It shows that these organizations are not in a mature stage of their CC adoption. Regarding the locus of decisions, Group 2 is divided between decentralized and centralized organizations. Organizations with a decentralized governance have their decision making process done through a collaboration between the different departments. Although they are still in a phase where they want to adopt cloud solutions, they either ignore the exact steps to follow or are afraid of a full 'cloudification'. This is where education, competences and skills play an important role. While they want to benefit from all the promised advantages, they are afraid of changes. Such organizations are on the right track towards cloud maturity and are prone to seek help from consulting companies that will guide them through the full transition. While their **Organization and Skills** maturity level is for most between 1.5 and 2, these organizations show a craving for learning, sharing their knowledge and pushing for more. They are on the correct path to implement cloud capabilities and increase their expertise in the near future. In addition, some have implemented cross-functional trainings for their employees (IT.12, IT.11, IT.18, IT.22, IT.4, IT.23, IT.21, IT.13). On the other hand, centralized organizations possess a low cloud maturity, probably due to the IT department being the sole decision makers. As discussed throughout this research work, CC engenders collaborations between the business and the IT departments as well as more communication, due to the agility of solutions. However, when the organization is centralized with the IT department as the decision maker, business departments will not be able to collaborate with them, or ask for specific needs. In addition, these departments will not be able to seek solutions with CSPs, as their IT department controls their budget. Therefore, the organization will stagnate instead of increase their cloud maturity. However, these IT participants seem "*satisfied with the current situation of the organization*" (IT.6), and do not wish to switch to a decentralized system (B.4, IT.23, IT.21, IT.13, IT.6). Instead, they choose to build their own private cloud. This case is understandable for some organizations, such as public ones. Their citizens' information is sacred, and they do not wish to store it in the public cloud, which explains this low maturity (IT.21, IT.6, IT.9, IT.10, and IT.20). While few are motivated by competition, the majority is divided between innovation and the reduction of costs, generated by CC. When asked about the strategy behind adopting cloud solutions, the majority of these organizations answered that due to the big financial advantage of cloud computing, they were pushed to adopt it. However, some others mentioned that innovation was their strategy; they needed to stay up-to-date and innovate.

**Group 3** represents six organizations with a very low cloud maturity (0.922 to 1.433). These organizations are in the initial level of adopting cloud solutions. They are still in the analysis phase, weighing the positive and negative aspects of CC according to their organization's needs and requirements. In addition, these organizations are all centralized, where four organizations are public (IT.19, IT.1, B.1, and B.3) and five organizations (IT.1, B.1, B2, B7 and B.3) are motivated by the reduction of costs. The IT department is the decision-maker for these organizations. Moreover, they only possess a few governance mechanisms implemented. All these factors, along with the fear factor, lead to the organizations' low cloud maturity. In addition, their employees lack skills and competences to deal with cloud solutions (**Organization and Skills** score of 1), which also influences the low level. Similar to some organizations of Group 2, these organizations are satisfied with such an adoption level, where some only adopt SaaS solutions.

**Table 29: Factors influencing cloud adoption intensity level**

| Ref. | Total Maturity Avg. (Table 28) | IT Governance | | | | Level of Competences | | | Corporate Strategy for CC adoption |
|---|---|---|---|---|---|---|---|---|---|
| | | Decisions (Table 21) | Locus of decisions (Table 22) | Decision Makers (Table 22) | Structures (S); Processes (P); Relational Mechanisms (R) (Table 23, Table 24, and Table 25) | Skills (Table 27) | Syndicates | Education System | |
| **IT.16** | 2,927 | Dep. Mod.; Serv. Mod.; Econ.; Secu.; Skills; Contract; Tech. | Decent. | Collab. (all dep. of different subsidiaries) | **S:** IT SC, CDO, CSO, Reporting; **P:** Gov Framework; **R:** AC, Shared Understanding | 3,333 | CGT; CFDT; CGT-FO; CFTC; CFE-CGC | French Education System | Competition |
| **IT.7** | 2,885 | Dep. Mod.; Serv. Mod.; Data; Skills; Contract | Decent. | Collab. with arbit. from the IT dep. | **S:** IT SC, Reporting; **P:** ITBC, Gov Framework; **R:** Communication, Cross-functional, AC, Shared Understanding, Partnership, Relation CSPs | 3 | | | Competition |
| **IT.24** | 2,813 | Dep. Mod.; Serv. Mod.; Trans.; CSP | Decent. | Collab. with arbit. from the IT dep. | **S:** CDO, Scrum Master; **P:** Scrum Methodologies; **R:** Communication, Cross-functional, AC, Partnership | 2,5 | | | Competition |
| **IT.5** | 2,526 | Dep. Mod.; Serv. Mod.; Trans.; Secu.; Contract; Tech.; CSP | Decent. | Collab. with arbit. from the IT dep. | **S:** CDO, CDPO, CSO, Scrum Master; **P:** Scrum Methodologies; **R:** Cross-functional, Partnership | 2,5 | | | Competition |
| **IT.8** | 2,302 | Dep. Mod.; Serv. Mod.; Secu. | Decent. | Collab. with arbit. from the IT dep. | **S:** CDO, DMC; **R:** AC | 2,5 | | | Competition |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **IT.12** | 2,276 | Dep. Mod.; Serv. Mod.; Why CC | Decent. | Collab. | **S:** CDO;<br>**P:** Gov Framework;<br>**R:** Cross-functional | 2,667 | | | Innovation |
| **IT.3** | 2,240 | Dep. Mod.; Serv. Mod.; Why CC; Econ.; Data; Policies | Decent. | Collab. with arbit. from the board | **S:** CDO;<br>**P:** Specific Processes;<br>**R:** Communication | 1,333 | | | Innovation |
| **B.9** | 2,219 | Dep. Mod.; Serv. Mod.; Secu.; CSP | Decent. | Collab. with arbit. from the IT dep. | **S:** CDO;<br>**P:** Gov Framework;<br>**R:** Communication | 2 | | | Innovation |
| **IT.14** | 2,156 | Dep. Mod.; Serv. Mod.; Econ. | Decent. | Collab. | **S:** IT SC, Purchasing Committee;<br>**R:** Communication | 1,833 | | | Innovation |
| **IT.11** | 2,135 | Dep. Mod.; Serv. Mod.; Why CC; Trans.; Secu. | Decent. | Collab. (all dep. of different subsidiaries) | **S:** LTC, IT SC, CDO;<br>**R:** Cross-functional | 1,667 | | | Innovation |
| **IT.18** | 2,134 | Dep. Mod.; Serv. Mod.; Secu. | Decent. | Collab. | **S:** IT SC, CDO;<br>**R:** Communication, Cross-functional | 2,167 | | | Innovation |
| **IT.22** | 2,115 | Dep. Mod.; Serv. Mod.; Why CC; Econ. | Decent. | Collab. with arbit. from financial dep. | **S:** Architecture Board;<br>**R:** Communication, Cross-functional | 2,333 | | | Competition – Reduction of costs |
| **B.11** | 2,104 | Dep. Mod.; Serv. Mod.; Policies | Decent. | Collab. with arbit. from the IT dep. | **S:** IT SC, CDO;<br>**P:** Specific Processes;<br>**R:** Communication | 2,333 | | | Reduction of costs |
| **IT.15** | 2,099 | Dep. Mod.; Serv. Mod.; Skills | Decent. | Collab. (all dep. of different subsidiaries) | **S:** IT SC, CDO, TAC;<br>**P:** Specific Processes;<br>**R:** Communication | 2 | | | Innovation – Reduction of costs |
| **IT.2** | 2,094 | Dep. Mod.; Serv. | Decent. | Collab. with | **S:** CDO; | 1,333 | | | Innovation – |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Mod.; Why CC; Econ. | | arbit. from the IT dep. | **R:** Communication, CSPs | | | | Reduction of costs |
| **B.6** | 2,042 | Dep. Mod.; Serv. Mod.; Trans.; Skills; Policies | Decent. | Collab. Especially with HR dep. | **S:** CDO, CDPO, CSO | 2,333 | | | Innovation |
| **B.10** | 1,979 | Dep. Mod.; Serv. Mod.; Why CC | Decent. | Collab. with arbit. from the IT dep. | **S:** IT SC, CDO | 1,833 | | | Innovation |
| **IT.4** | 1,927 | Dep. Mod.; Serv. Mod.; Customer | Decent. | Collab. with arbit. from IT dep. | **S:** IT StC; **R:** Communication, Cross-functional, AC | 1,667 | | | Reduction of costs |
| **B.4** | 1,844 | Dep. Mod.; Serv. Mod.; Customer | Cent. | IT dep. | **S:** CDO; **R:** Communication, Cross-functional | 1,667 | | | Innovation - Reduction of costs |
| **IT.23** | 1,823 | Dep. Mod.; Serv. Mod. | Cent. | Collab. with arbit. from the IT dep. | **S:** IT SC; **R:** Communication, Cross-functional | 1,833 | | | Innovation |
| **IT.21** | 1,771 | Dep. Mod.; Serv. Mod. | Cent. | IT dep. | **S:** CoC; **R:** Communication, Cross-functional | 2 | | | Reduction of costs |
| **IT.13** | 1,755 | Dep. Mod.; Serv. Mod.; Skills | Cent. | IT dep. | **S:** CoC; **R:** Communication, Cross-functional | 1,833 | | | Reduction of costs |
| **B.8** | 1,714 | Dep. Mod.; Serv. Mod.; Econ. | Cent. | IT dep. (some discussions with CEO) | **S:** CDO; **R:** Communication, Cross-functional | 1,5 | | | Innovation - Reduction of costs |
| **IT.6** | 1,708 | Dep. Mod.; Serv. | Cent. | IT dep. | **S:** IT SC; **P:** Gov Framework; | 2 | | | Reduction of costs |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Mod.; Data | | | **R:** Communication, Cross-functional | | | | |
| **IT.17** | 1,661 | Dep. Mod.; Serv. Mod. | Decent. | Collab. with arbit. from the board | **S:** CDO;<br>**R:** Communication | 1 | | | Innovation - Reduction of costs |
| **IT.9** | 1,646 | Dep. Mod.; Serv. Mod.; Data | Cent. | IT dep. | **S:** CEDO;<br>**R:** Communication, Cross-functional | 1,333 | | | Innovation |
| **IT.10** | 1,635 | Dep. Mod.; Serv. Mod.; Data | Cent. | IT dep. | **R:** Communication, Cross-functional | 1,5 | | | Innovation |
| **IT.20** | 1,547 | Dep. Mod.; Serv. Mod.; Data | Cent. | IT dep. | **P:** Gov Framework;<br>**R:** Communication | 1 | | | Innovation |
| **B.5** | 1,536 | Dep. Mod.; Serv. Mod. | Decent. | Collab. with arbit. from the IT dep | **S:** IT SC;<br>**R:** Communication | 1,5 | | | Reduction of costs |
| **IT.19** | 1,443 | Dep. Mod.; Serv. Mod.; Data | Cent. | IT dep. with accordance with Prime Minister | **S:** CDO;<br>**R:** Communication | 1,167 | | | Innovation |
| **IT.1** | 1,229 | Dep. Mod.; Serv. Mod.; Secu. | Cent. | IT dep. | **S:** Scum Master, Data Mining Expert;<br>**R:** Communication | 1,333 | | | Reduction of costs |
| **B.1** | 1,177 | Dep. Mod.; Serv. Mod. | Cent. | IT dep. | **S:** IT StC;<br>**R:** Communication | 1 | | | Reduction of costs |
| **B.2** | 1,146 | Dep. Mod.; Serv. Mod. | Cent. | IT dep. | **S:** IT SC, IT StC | 1 | | | Reduction of costs |
| **B.7** | 1,000 | Dep. Mod.; Serv. Mod. | Cent. | IT dep. | **R:** Communication | 1 | | | Reduction of costs |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **B.3** | 0,922 | Dep. Mod.; Serv. Mod. | Cent. | IT dep. | **R:** Communication | 0,833 | | | Reduction of costs |

**Legend: Decisions:** Trans.= Transition; Dep. Mod.= Deployment Models; Serv. Mod.= Service Models; Econ.= Economics; Secu.= Security; Data= Data Stored; Skills= New Skills; Contract= Cloud Contracts; Tech.= Technical Transition; CSP= CSPs Relationships; Customer= Customers Relationship.

**Locus of Decisions:** Decent.= Decentralized; Cent.= Centralized.

**Structures (S)**: IT SC= IT Steering Committee; CDO= Chief Digital Officer; CDPO= Chief Data Privacy Officer; CSO= Chief Security Officer; DMC= Data management committees; TAC= Technical Architecture Committee; LTC= Legal and Technical Committee; IT StC= IT Strategy Committee; CoC= Center of Competency; CEDO= Chief Exchange and Digital Officer;

**Processes (P)**: ITBC= IT Balanced Scorecard Reporting= CIO and CEO report to the board; Gov Framework= Governance Framework (COBIT, etc.);

**Relational (R):** AC= Awareness Campaign; Communication= communication between IT and Business departments; Cross-functional= Cross-functional business and IT job rotations and training; Partnership= Partnership rewards and incentives; Relation CSPs= Relationship with CSPs.

# VI. Cloud Governance Framework

After analyzing the results from part I and part II and based on Table 29, we gathered all these information to build a cloud governance framework. Drawing on these results, our framework represents the different factors affecting an organization's IT governance, adapted to cloud services, and its intensity level of cloud adoption ('Cloud Maturity'), as presented in Figure 35.

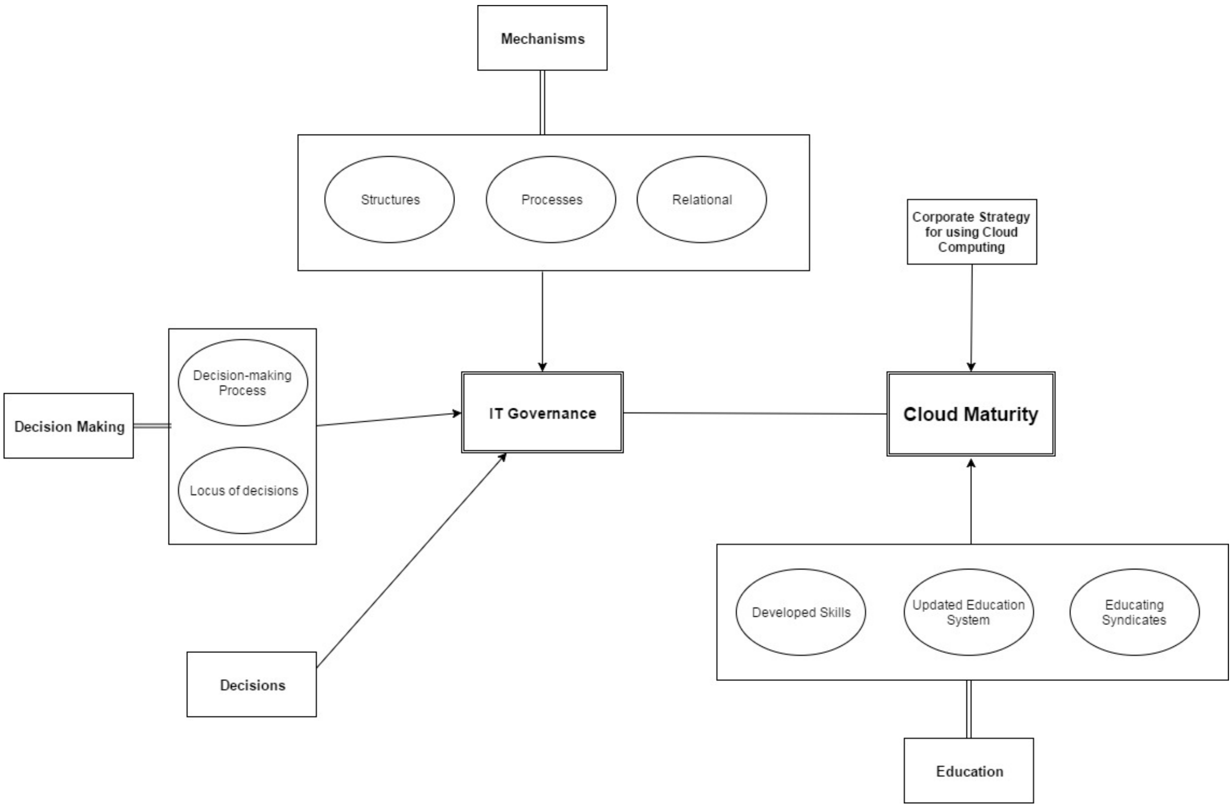


**Figure 35: Cloud governance framework (source: the author)**

Cloud maturity can be affected by two factors according to our results; the corporate strategy of the organization for adopting cloud solutions, and the level of education/skills/competences the employees possess related to cloud subjects. Regarding the first factor, Table 29 showed that organizations, having competition as a motivation to keep their places in the fast-growing competitive market, are pushed to work on increasing their cloud maturity, and hence on adopting cloud services that are used by their competitors. Unlike these, organizations that simply want to adopt CC to reduce their costs possess a lower cloud adoption. Such organizations do not focus on their cloud maturity; instead, they emphasize the financial benefits generated by CC on the short term (as shown in Table 29). Furthermore, based on the literature, CC is a new type of service that demands new competences and new skills. These are developed through training sessions in the organization or at an earlier stage of the employee's life, through dedicated classes at the university. Therefore, the more skills and competences employees possess, the easier the cloud adoption is. It is also important to ensure that syndicates are on board regarding the adoption of cloud services in order to avoid any opposition. This factor can slow or even inhibit the adoption process where the influence of syndicates weighs heavily on the organization. Thus, developing employees' skills, implementing innovative syllabi, and educating syndicates are important for the intensity level of cloud services adoption.

Based on the results from Part I and Part II, the effective IT governance of organizations, adapted to cloud technology, is dependent on several factors: the cloud-related decisions addressed during the decision-making process, the locus of the decisions, the decision makers allocated to the cloud-related decisions while focusing on the role of the IT department in the decision-making process, and finally the adoption level of governance mechanisms. Decisions taken related to CC adoption affect the organization's intensity level of cloud services adoption. During the board or committee meetings, numerous of decisions are made daily. However, when implementing CC, the executives need to redirect their focus and priorities on decisions related to the adoption of cloud solutions. Organizations should take into account vital decisions that will mostly have an impact on their cloud maturity levels, such as "New Skills", "Cloud Contracts", "CSPs Relationship", "Policies" (Retrieved from Table 21). The rest of the fundamental cloud decisions are represented in Table 21. Nevertheless, in order to make these decisions, appropriate decision makers need to be allocated responsible for different decisions. Based on our results, having a centralized governance leads to different cloud maturity levels than having a decentralized one. For instance, as shown in Table 29, the cloud maturity level is lower for organizations having the IT department as the cloud-related decision makers, compared to decentralized organizations. In addition, the decision-making process influences the level of adoption of cloud services, where the role of internal IT is very important in the decision process. For instance, a high input or no input from the IT department does not increase the cloud maturity level of the organization. The IT department should not take all the decisions by itself, nor should it leave the decisions for the business departments. On the other hand, while CC engenders agility, and hence communication and collaboration, the IT department is advised to collaborate with the business departments in order to instore an optimal cloud adoption level. To complete the IT governance, organizations are advised to implement governance mechanisms as decision-making structures, business processes and relational mechanisms. It is through structure mechanisms that organizations are going to allocate decisions to the appropriate decision makers. In addition, being a new technological asset for the organization, CC needs to have policies defined in order to instore daily behaviors for employees, which is done through adopting business processes. Finally, relationships between employees have to change with CC. Therefore, implementing fundamental structures, processes and relational mechanisms that will deal with the adoption of cloud solutions is primordial for the cloud maturity level, as shown in Table 29. For instance, the high number of adopted mechanisms was one factor affecting the high cloud maturity level of Group 1, compared to Group 2 and Group 3. After improving these three factors (decisions, decision makers, and mechanisms), organizations will possess a higher intensity level of cloud services adoption.

According the analysis of Part II, we have notice a correlation present between the intensity level of cloud services adoption and the effective IT governance of cloud solutions. For instance, the higher the intensity level is (‘cloud maturity’), the more effective the IT governance is (higher level of governance mechanisms, for instance) and vice versa.

## VII. Governance Models

Based on the three groups of organizations classified in Table 29, different governance models emerged, which will be presented in this section. The number of mechanisms adopted, the locus of the governance, the decision makers, the number of decisions addressed, and the developed skills constitute emerging factors of the governance models.

Organizations of Group 1 are all decentralized, where the decision-making process goes through collaborations between the different departments. Similarly, organizations of Group 3 are all centralized, where the IT department makes the IT-related decisions. In addition, the number of mechanisms adopted by organizations, the number of decisions and the developed skills vary. Therefore, to build a governance model that represents each group, we had to calculate the average values of these factors. We, hence, calculated the average number of mechanisms adopted by each Group (Group 1 and Group 3), the average number of decisions addressed, and the average skills maturity. However, Group 2 is divided into centralized organizations and decentralized one. Therefore, two governance models represent this group. We proceeded the same way in order to get the different factors.

Four different types of governance models emerged from our results. The first model illustrated in Figure 36 represents the governance of organizations that belong to the Group 1, having an intensity level of cloud services adoption of CMM3. Based on our results, organizations having a cloud maturity level of CMM3 adopt on average 7 governance mechanisms (whether decision-making structures, business processes, and/or relational mechanisms). It is important to notice that these organizations varied the governance mechanisms implemented, and adapted them to match cloud requirements. Additionally, they have a decentralized governance where the IT and cloud-related decision-making process happens through collaboration between different departments, and the average number of decisions discussed is 5 important cloud decisions. Finally, it appears that these organizations have an average skills maturity of 2.8 over 5; meaning even if their employees are developing strategic skills, their cloud-related expertise is still not optimal.

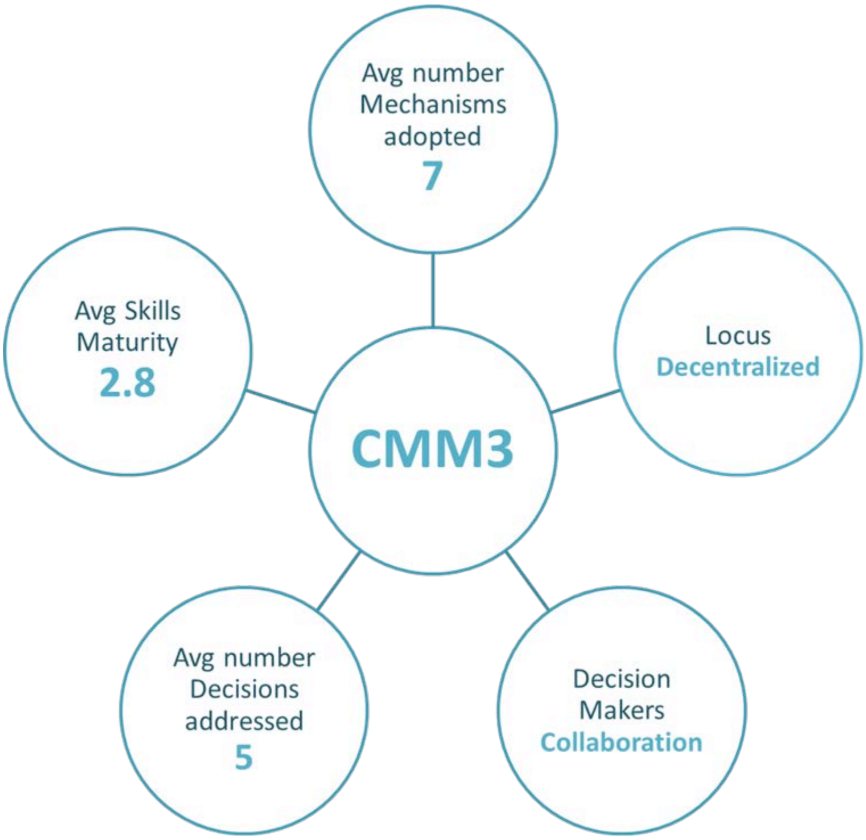


**Figure 36: Governance model for Group 1 (CMM3)**

The second model illustrated in Figure 37 represents the governance of decentralized organizations belonging to the Group 2 and having an intensity level of cloud services adoption of CMM2. Based on our results, decentralized organizations having a cloud maturity level of CMM2 adopt on average 3 governance mechanisms (a small variation of decision-making structures, business processes, and/or relational mechanisms). As they are decentralized, decisions are made through collaboration between the different departments, while discussing on average 3 cloud-related decisions. Finally, it appears that these organizations have an average skills maturity of 1.9 over 5; their employees are gradually updating their cloud competences.

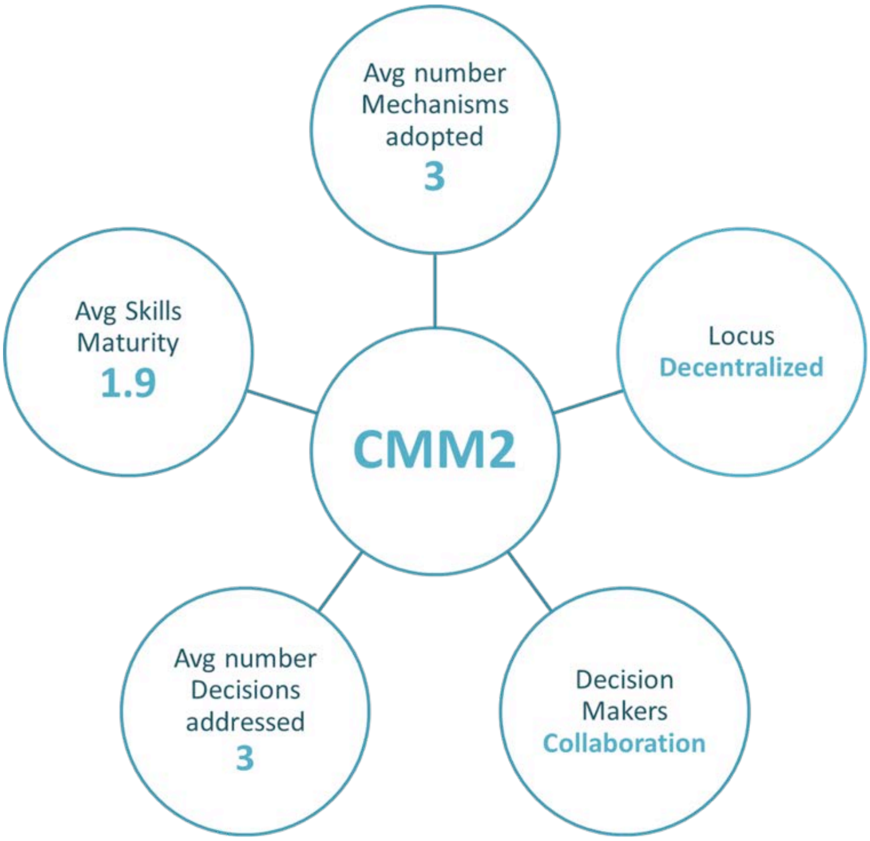


**Figure 37: Governance model for Group 2 (CMM2 decentralized)**

The third model illustrated in Figure 38 represents the governance of centralized organizations belonging to the Group 2, having an intensity level of cloud services adoption of CMM2. Based on our results, centralized organizations having a cloud maturity level of CMM2 adopt on average 2 governance mechanisms that are not varied. Additionally, the IT department makes the IT and cloud-related decisions, while discussing an average of 2 cloud decisions (usually regarding the deployment and service models). Finally, it appears that these centralized organizations have an average skills maturity of 1.6 over 5; their employees are learning more about cloud computing and trying to apply their knowledge.

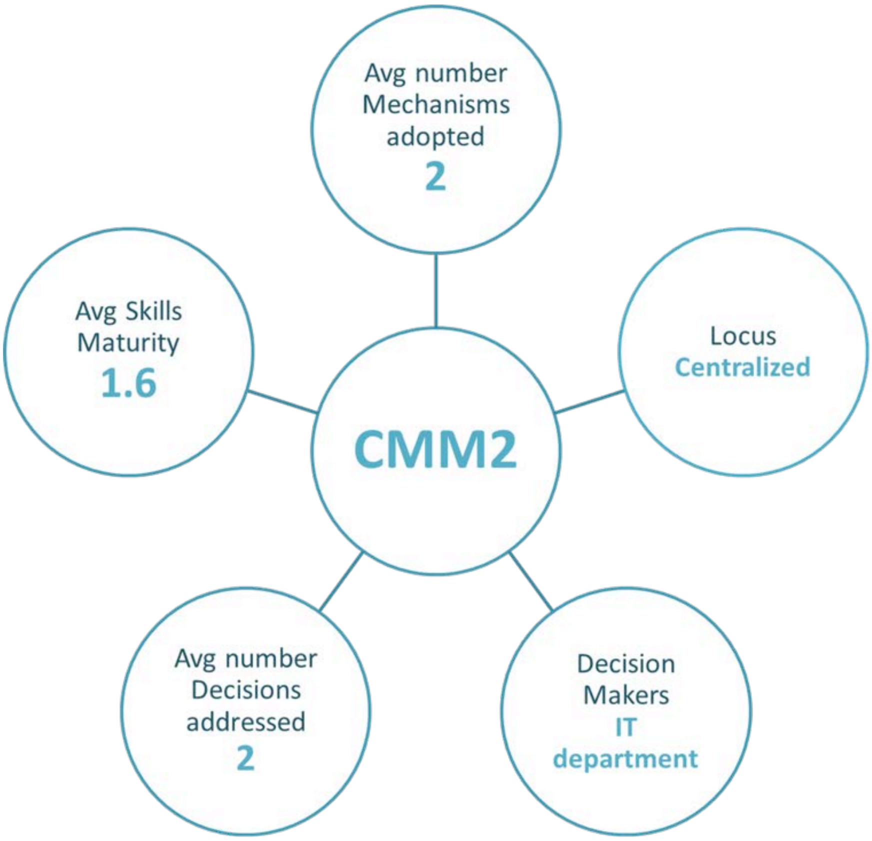


**Figure 38: Governance model for Group 2 (CMM2 centralized)**

The last model that emerged from our results is illustrated in Figure 39 and represents the governance of organizations belonging to the Group 3, and having an intensity level of cloud services adoption of CMM1. These organizations adopt on average 1 governance mechanism; they are not familiar with cloud governance mechanisms or they do not see the use from implementing cloud governance mechanisms. Furthermore, the IT and cloud-related decisions are solely made by the IT department, while discussing on average 2 decisions (mainly the deployment and service models to adopt). Lastly, these organizations have an average skills maturity of 1.0 over 5, representing a low level of skills in cloud services.

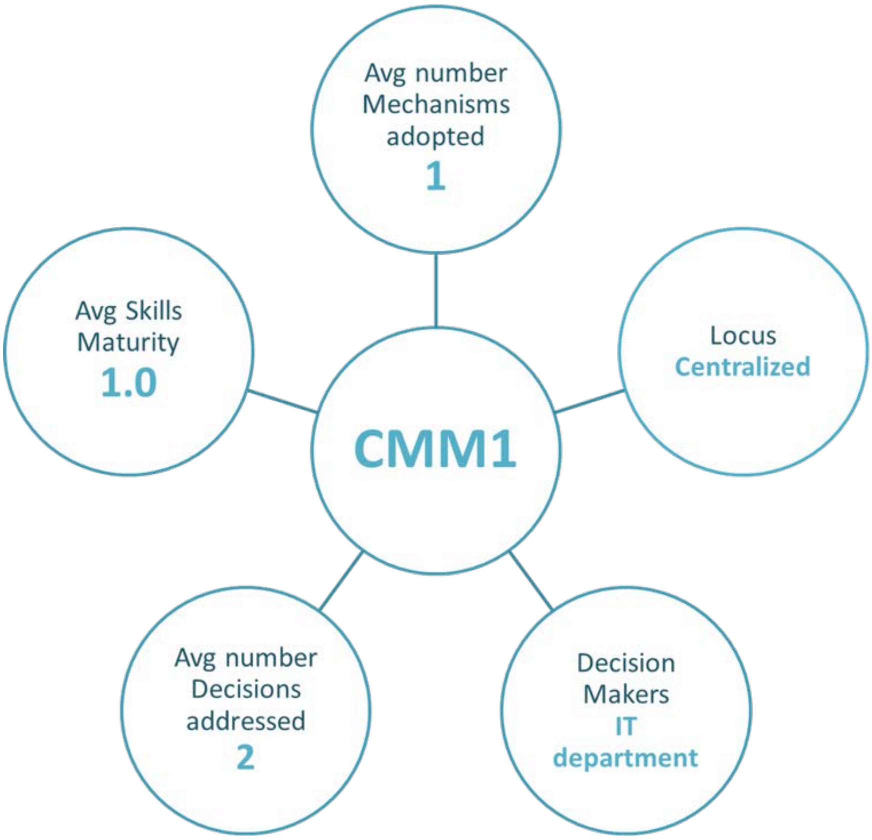


**Figure 39: Governance model for Group 3 (CMM1)**

# Discussion

This chapter discusses the data analysis from both rounds of interviews. It starts by discussing the findings related to the reasons leading organizations to govern their cloud services and the way they need to do it. It also discusses how cloud governance affects the intensity level of cloud adoption within organizations. Due to the various transformations generated by cloud solutions in organizations, the author presupposed that IT governance models aren’t sufficient for governing cloud services. Before getting to the cloud governance characteristics that can help organizations (including a competitive advantage, lower costs, better performance, etc.), the author discusses the findings that shed light on the impacts of cloud solutions that should be taken into consideration by organizations. Data findings mostly revealed transformations in the IT skills and roles due to the changes in IT infrastructure, processes, and project management methodologies.

After discussing the different results that emerged in the previous section, the discussion chapter states the various limitations of this research work. In addition, future research is discussed, addressing several opportunities for more developed research. The author ends this chapter by emphasizing the novelty of this research and the numerous contributions to the academic and professional literature.

# THE WHY

## I. Cloud Adoption and Change Management

Cloud computing is transforming IT infrastructures in organizations. Hence, new decision types as well as new service purchasing strategies have emerged. Before adopting cloud services, the IT department installed servers and routers, connected cables, developed applications on their own infrastructures. The emergence of cloud computing has changed this traditional role into a role where IT departments are in charge of monitoring information technologies by pushing a few buttons from their desktops, along with purchasing the most suitable cloud services. Hence, they are accountable of effectively benchmarking the right cloud service providers and negotiating contracts with them. In addition, they must decide on whether to internally develop applications, adopt cloud services privately or publicly. As a result, new skills in benchmarking, negotiation, contracts and finance need to be acquired by IT departments in order to take the right decisions that optimize the costs and return on investments of cloud services. Through these new skills adapted to cloud technologies and hence through their effective governance, IT departments will be capable of providing better input regarding services acquisition.

Cloud services have also modified the relationship between business units and the IT department. Due to the flexible nature of the cloud, business units are capable of adopting cloud services independently, without the help of their IT department. In such circumstances, IT departments are urged to become proactive and oriented towards business needs as they have no longer a monopoly on IT. This change of perspective has largely affected the required skills of IT departments in large organizations. In addition to staying up-to-date with the latest technological innovations, IT departments need to be aware of the market and business evolving needs. This is essential in order to maintain control over IT services in organizations, their costs and risks. Yet, even with the development of their market understanding, IT departments need to involve business units in their cloud decision-making process to improve the alignment between the business and cloud strategies. Based on the Henderson and Venkatraman model, organizations need to implement cloud services that support their strategies. Aligning the different business and IT needs is primordial within organizations aiming for success. The strategic alignment model proposed by Henderson and Venkatraman (1989) has been widely discussed in the IS literature and applied by organizations to integrate their business and IT, enhance the competitiveness and improve firm performance. In addition, organizations' top management and innovation teams understand that a successful introduction of digital technology, such as cloud computing, combines information and skills available with new technology capabilities in order to create new solutions and improve operations.

Cloud computing has also introduced new ways of dealing with the organization's security affecting the required skills of IT departments. While IT security teams used to monitor their security through various tests during the legacy, the emergence of cloud computing shifted these tests towards contractual monitoring. Thus, decision makers have to control the organizations' contracts with their cloud service providers, ensuring that they cover the required standards of the cloud services security aspects. In addition, decision makers must ensure the reliability of these contracts, monitoring the various clauses according to the organization's regulations. In accordance with the literature, cloud contracts must include clauses ensuring the data privacy of the customers. This links us back to the need of identifying and acquiring new skills that enable IT departments to deal with cloud contracts.

Furthermore, the adoption of cloud computing is affecting the structure and management models in organizations. Hence, numerous organizations tend to break their traditional models, based on "rigid" project management methodologies and policies. In fact, traditional "models" – such as waterfall and "V" cycle models – have been increasingly questioned for the last two decades, even before the adoption of cloud solutions. These models are perceived as unable to cope with rapid changes, evolving technologies and customer changing demands (Standish Group, 2015; Poppendieck, 2006; Highsmith and Cockburn, 2001). Thus, a new set of "lightweight" methodologies, known as "agile" methodologies, has gained attention among practitioners and organizations. These methodologies are based on iterative development, close collaboration, continuous integration and adaptation to changes. Yet, the implementation of these management principles and practices isn't always easy to achieve. Many contextual factors such as team distribution, project manager's authority, organizational structure and culture seem to constrain the creation of an agile environment (Khalil and Fernandez, 2013). However, the "flexible" nature of cloud solutions help organizations overcome these challenges and become agile. According to our participants, there's a change in the mindset of IT project teams who are dealing with cloud solutions. Cloud services push large and distributed teams on becoming closer by communicating and collaborating more. By providing access to secured online documents and enabling remote connection, development on virtual platforms, pair programming as well as continuous integration, cloud computing helps distributed teams overcome many development-related challenges. This triggers the creation of an agile environment. Furthermore, the adoption of cloud solutions has led to the creation of more agile structures and roles – the integration of the scrum master role for instance. In addition, by its ubiquitous nature, cloud computing has enhanced teleworking and telecommuting practices. In a cloud environment, employees can work, code, share documents, run meetings from anywhere in the world "*we possess 10.000 employees who are teleworking – working from outside their offices*" (IT.24). As data analysis shows, adopting cloud services is perceived to be helpful for the agility of organizations, allowing them to benefit from the opportunities of agility while solving its challenges. In this respect, cloud solutions can be viewed as an instrument that supports the creation of an agile environment. They help IT project teams in becoming more adaptive to business changing needs.

The adoption of cloud services has also led to new ways of working and managing employees. By enabling teleworking, managers are facing new challenges regarding controlling their employees' work and presence at work. Whereas this can be perceived as a threat to the managers' position and authority, organizations need to change their policies and encourage their managers to also change their leadership.

Due to the major changes that cloud technology trigger in organizations, the adoption of cloud services needs to be viewed as a change management project that involves different stakeholders. Organizations therefore need to deploy change management in order to facilitate their transition (and specifically of their employees) towards cloud services. Change management is an organizational term 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 and Brightman, 2001, p. 111). Change management is a completely natural and normal reaction to the different internal conditions that the organization goes through (Leifer, 1989). For the past decades, it has been considered as a necessity for organizations to evolve and succeed in today's competitive market (Luecke, 2003; Okumus and Hemmington, 1998). Organizations support their employees' capability to undergo continuous change according to the transformations witnessed within the organizations. Therefore, it is a natural response for employees to change when their organizations decides to adopt cloud services.

First, organizations need to identify the different stakeholders that are involved in the adoption process of cloud services and analyze their contribution to the change project (Moir, 2001). The stakeholder analysis will consist on identifying the primary stakeholders, analyzing their needs, expectations, power, and influence. According to this stakeholder analysis, organizations will be able to define the right actions that need to be implemented in order to decrease resistance regarding the changes that are related to the adoption of cloud solutions. Our data findings revealed, for instance, a primary stakeholder that wasn’t mentioned in literature, and that needs to be taken into account while adopting cloud services: syndicates. This can be explained by the organizational culture of French organizations where syndicates play a significant role. Being the voice of employees, their aim is to protect employees from any change that may affect their social security and safety at work. According to our participants, syndicates perceive cloud solutions as a threat to the IT staff positions. As syndicates seem to be against the adoption of cloud solutions, it is essential to deploy the right communication plans, highlighting the benefits that IT employees obtain from adopting cloud services. Therefore, it is fundamental to educate them and have them on board with the organization’s digital transformations. In addition, organizations are advised to sign agreements with their syndicates regarding the digital transformations affecting them, as noted by IT.16 where “*this agreement aims at raising awareness regarding the possibility of teleworking, for example*”.

This stakeholder analysis needs to be followed by defining and implementing the right training and communication programs. Along with the top management, IT and business managers’ support, the HR as well as the communication departments play an important role in conducting changes in organizations that are adopting cloud solutions. While the HR department participates in redefining IT roles, identifying the appropriate training and integrating these trainings to the HR policies, the communication department assists the top management in defining communication plans and adapting them to each audience of the organization. Training sessions, communication, and coaching should support the change in mindset throughout the organization while adopting cloud technology. Furthermore, implementing key performance indicators that highlight “short-term wins” can be beneficial for increasing the adoption of cloud services and embracing changes.

Hence, the change management concept is highly critical when addressing cloud-related transformations. Organizations need to slowly bring changes to employees by "*discussing the need of these changes as well as the way to evolve*" (IT.6). While cloud computing influences the way IT is managed in an organization, change management seems indispensable. Thus, through change management, organizations that adopted cloud services can evolve in maturity. Plus, every change affecting the organization needs to be listed along with its consequences, and a plan to manage them. This is what classifies change management as particularly important. In addition, abruptly telling some employees that, for example, their jobs will disappear and will be replaced by new services is not the correct way to introduce changes. Therefore, organizations need to put a lot of effort and time in educating employees and anticipating new needs. This shows the link between developing skills and the need for change management. Additionally, cloud computing has an impact on human resources of the IT department specifically. The question that organizations ask is what to do with their IT employees' competences. When an organization has many employees that are relatively old, it becomes problematic when adopting cloud services. On one side, it will be hard to train them on new subjects at the end of their careers. On the other side, due to some firing policies stated by the French law, organizations are unable to fire them under the pretext that they lack skills adapted to cloud computing. Not being able to develop their employees' needed skills is "*one of the reasons [organizations] are still not are fully immersed in the whole cloud universe*" (IT.6).

## II. Cloud Adoption and Risk Management

With the adoption of cloud services, risk management becomes critical for organizations, as this new technology engenders several threats. For instance, many risks associated with cloud technologies are highlighted in the data analysis. They include data leaks, outsider attacks, data loss, vendor lock-in, compliance to national laws, etc. These risks were also evoked in the literature.

Dealing with cloud contracts seems to be an important issue for organizations deploying cloud services. Therefore, developing skills in reading the different contract clauses is primordial for employees before subscribing to any cloud service. From the long list of clauses in a cloud contract presented in the literature, our analysis highlights three main clauses: the reversibility, confidentiality and SLA clauses. First, organizations need to feel safe about having their data written in a universal programming language and being able to use it on different platforms. Then, due to the strict compliance laws in France, organizations need to be reassured of the confidentiality of their data once saved on their provider's cloud. Finally, as highly mentioned in the literature, organizations are strict about the reliability and the quality of the solutions they adopt. These clauses, emphasized by the literature and our participants, play an important role in the adoption process of cloud services.

These security laws arose from the high value of organizations' data and their need for protection, after various security breaches and many data leaks incidents. While data security and privacy are becoming critical issues for organizations adopting cloud services, cloud service providers understand that reassuring their customers regarding the privacy and security of the stored data would give them a competitive advantage. This highlights the importance of signing appropriate cloud contracts stating the various primordial clauses (such as, data protection, data privacy, SLAs, etc.). Moreover, data privacy should not hold back organizations from implementing and adopting cloud services. In today's competitive market, the various cloud benefits are too important to disregard adopting cloud services due to some privacy regulations. In accordance with the literature and the data analysis, the CNIL should reinforce their supervision and protection of the data stored in France, in order to reassure French organizations and push them to increase their intensity level of cloud services adoption.

In addition, a key relationship is also built through cloud services. Cloud service providers represent a critical part of the cloud computing ecosystem, according to a large state of the art. Moreover, CSPs are necessary stakeholders for the interviewed organizations. An important relationship is built between the organization and its CSPs, based on trust, respect, and reciprocity. Missing one of these would lead to breaching the cloud contracts. This would hurt both parties; on the one hand, the CSP's reputation will be jeopardized, and on the other hand, the organization's data on the provided service are prone to be lost. Choosing the most appropriate cloud service providers is not an easy task. According to the data analysis, CSPs are expected to possess sufficient funds to provide services over the long term (at least over the contract length). CSPs are more attractive to organizations when they are in a healthy fiscal stable position. While establishing risk management policies is a key characteristic of cloud contracts offered by CSPs, the latter is expected to validate compliance with the various requirements set by the organization and audited by a third party. Even if "*it has become* *extremely hard to audit fairly the CSP*" (IT.8), organizations are advised to trust the third-party audit before signing any contract with the audited CSP. As previously mentioned, trust, respect, and reciprocity play an important role in evaluating CSPs. Their reputations (through reviews, previous audits, ratings) should also be characteristics verified by organizations before buying cloud services. Finally, the data analysis highlighted the importance of the business and technical expertise of CSPs in order to communicate with the different employees and fulfill their needs. In order to ensure an appropriate decision regarding CSPs, organizations are required to know these details that seem to be missing from the academic literature.

Along with these risks, new ones emerged from our data analysis such as the risk of being too dependent on suppliers. Many participants emphasized the dependency of their organizations on cloud service providers. Thus, their organizations undergo manipulations related to the price of cloud solutions or CSPs' audit activities. In addition, they lack long-term guarantees of the adopted cloud services.

Shadow IT is another risk that has been highlighted in the data analysis. Our findings revealed that perceptions regarding shadow IT aren't incongruent. While some groups of participants perceive shadow IT as a risk, others consider it as a "normal" existing practice.

Business managers perceive shadow IT as a common business practice. All business participants acknowledge that their departments mostly "*buy software solutions from [cloud] providers*". According to business managers, shadow IT links back to the benefits generated by cloud services, such as agility ("*The business departments are moving fast, with more work and short deadlines, due to the fast-moving market. So it is understandable that [business departments] get the solution the minute they need it*", IT.24), and performance ("*The communication department needed to store 50 Terabytes of video files […] and they searched for providers offering large storage capacities and a good quality*", B.9). With the presence of various offers from cloud service providers, business units do not need the IT department to develop a required application ("*I do feel that the IT department is no longer in total control of the organization, especially with the presence of all the different cloud solutions offered by providers*", B.11). Business managers "*feel [they] possess new powers through the cloud*" (B.2) and that "*the IT department is no longer in total control of the organization*" (B.11). As reasons for this perceived general development in which governance is shifting, they cite the lack of responsiveness of IT departments who are "*not able to fulfill all sorts of* *needs today*" (B.5). Even an IT department that "*tries to take the initiatives and be proactive*" (B.6) according to their views, will not be able to fulfill their "*business departments' need [for] specific software*" (B.6), which links again to their benefits frames of increased performance.

However, according to some of IT managers, shadow IT either does not occur or just at a very limited scale. The IT stakeholders cite different reasons for why they see this phenomenon as rare, for example since "*business departments do not have the budget*", "*it is [the IT department] that controls IT*" (IT.6). IT stakeholders are convinced that responsiveness and a culture of being a "*more discussion-kind of organization*" (IT.24) help in addressing potential shadow IT issues: "*I don't think shadow IT is a huge problem in our organization, of our policies, stating that we build together with the business department, so if they need anything, we are here for them*" (IT.8); "*our IT expertise is still required*" (IT.12). But for those who acknowledge the existence of shadow IT, they heavily emphasize the risks, linking back to the threats brought by cloud computing ("*Shadow IT is really dangerous. Especially when business departments do not pay full attention to the CSP trustworthiness, the quality of their services, and particularly to the security issues*", IT.11).

In fact, in the minds of IT managers, their exertion of governance and control should be strengthened to prevent business units from using cloud IT in the shadows. There is a strong mental liaison to the idea that "*the IT department controls anything related to IT*" (IT.19) and that business "*departments need to get the [IT department's] permission before seeking solutions from cloud providers*" (IT.10). Some are willing to grant business units "*small budgets to buy software that is not harmful*" (IT.23), but generally business departments "*are not allowed to go behind and contact cloud providers on their own*" (IT.20).

Therefore, adopting cloud services not only impacts organizations through increasing the presence of shadow IT practices, but it also drives them to redefine their IT governance. On one side, business managers can use shadow IT practices as a reason to become independent from their IT department, changing their IT governance structure. On the other side, the inherent fear of losing governance and control may blind IT stakeholders of the existence of shadow IT, which also jeopardize the governance of cloud services.

Hence, stakeholders have different perceptions regarding shadow IT practices. As they have divergent objectives, perceptions and expectations, conflicts of interest between stakeholders tend to rise in organizations adopting cloud solutions. Once again, a stakeholder analysis is fundamental in order to find ways to help organizations converge their stakeholders' visions and interests.

Conversely, there is substantial evidence that several benefits are associated with cloud computing. Our findings converge with many aspects of cloud computing found in the academic literature. As mentioned in the state of art, a proper integration of cloud computing provides cost savings that come from economy of scale, scalability and lower resource consumption. Everything moves extremely fast in the digital age. Organizations are hence advised to be agile and innovative. Thus, employees are pushed to work in an agile project mode, in communities, and from different places. Cloud services also improve time-to-market, process agility, service quality as well as employees' autonomy. Nonetheless, our findings highlight some other specific benefits that were less portrayed in the literature. Our respondents evoked cost savings that come from the lack of updates and the lower servers' downtime. In addition, our respondents viewed cloud computing standardization as a benefit whereas in the literature this characteristic is considered as a threat, affecting enterprises' competitiveness. This leads us to reflect that the deployment process of the right standardized CSP's offers mainly affects the organization's competitiveness. In other words, it is more what the organizations do with the standardized cloud services and how they align them to their organizational and business needs that enable them to gain a competitive advantage.

While aligning cloud services with the business strategy and the organization infrastructure helps the organization benefit from the promised advantages, adopting such services is still challenging. In fact, business managers essentially anticipate that the internal distribution of IT decisions-making power will need to be redefined in a way that business units take stronger governance, and IT units will lose control.

As a result, organizations do not fully or optimally adopt cloud solutions even when changes are conducted properly. Hence, governing the cloud appears to be essential. This is central if organizations aim at evolving in maturity and reaching the optimal cloud maturity level.

# THE HOW

## I. Governing Cloud Services

We have seen that no governance model addressing the various angles of cloud computing exist in the literature. Even though some participants mentioned the adoption of various parts of governance frameworks, such as COBIT and ITIL, these do not seem to be the most suitable for governing cloud services. Therefore, this pushed us to explore the way to govern cloud services and whether they actually need specific IT governance. In order to explore the specific governance characteristics needed by cloud services, we based our research work on the IT governance defined by Luftman and Brier (1999), Sambamurthy and Zmud (2000), Peterson (2004), and Weill (2004) (focus on making decisions and allocating the different decision makers through the use of governance mechanisms). According to the data analysis, several aspects emerged proving the need for specific governance when implementing cloud computing.

Regarding cloud-related decisions, they are not addressed by researchers. Nonetheless, based on the answers received by the interviewed participants, a large number of decisions are discussed and tackled before the adoption of cloud services. Therefore, decision makers will have to incorporate cloud decisions along with their IT ones, as the first step of governing these services. However, cloud-related decisions do not completely fall under the 5 major IT decisions mentioned in the literature (IT principles, IT architecture, IT infrastructure strategies, business application needs, and IT investment and prioritization). Based on the analysis of our results, we can therefore classify cloud-related decisions under 5 key groups; transitions, issues to solve, types of models, cloud service providers, and cloud policies. Decisions related to transitions represent the different steps to consider before and during the merge to the cloud. Organizations need to also be aware of the different issues and risks engendered by cloud services. Therefore, such critical decisions need to be addressed and taken into account. They also have to decide which deployment and service models to adopt. Regarding the cloud service providers, organizations should choose the most appropriate and reputable providers along with the most suitable cloud contracts. Finally, cloud policies consist of a set of policies and standards required for a correct implementation of cloud services. Thus, organizations willing to adopt cloud services can start their transition by addressing the five identified categories regarding cloud decisions. The previously mentioned decisions are interrelated and are prone to affect one another. Therefore, it is important to prioritize decisions that are critical for the organization (whether it is related to the security issues, the data storage possibilities, the types of cloud to migrate to, etc.). Prioritizing cloud-related decisions allow organizations to make the most suitable decisions that are aligned with the business strategy of the organization.

After addressing these cloud-related decisions, governing cloud services consist of allocating these decisions to the most appropriate decision makers. Nevertheless, behind the simplistic façade of the decision-making process, it is a complicated task. Many authors divided the decision making process into two parts (decision control rights and decision management rights) while others (Xue et al. 2008) noted that IT governance should include pre-decision stages stressing that the participants are more important than the final decision makers. This represents a limitation of our research work where we only explored the decision making process as a holistic matter.

As affirmed by Tiwana (2009), generally, the IT department is responsible for taking the decisions when IT governance is centralized, and when it is decentralized it becomes the business departments' responsibilities. This argument is supported by our 35 organizations. For instance, the IT department is the decision maker in most of these centralized organizations (B.1, B.2, B.3, B.4, B.7, B.8, IT.1, IT.6, IT.9, IT.10, IT.13, IT.19, IT.20, IT.21) where, only in a few cases, decisions where mainly made by the IT department with the agreement of other instances (the prime minister). From the different decision makers archetypes suggested by Weill and Ross (2004), the IT monarchy archetype is present in these centralized organizations. From the other archetypes proposed, the IT duopoly one (when business employees need cloud solutions it gets communicated to the IT department for a final arbitration) emerges as well (B.5, B.9, B.10, B.11, IT.2, IT.4, IT.5, IT.7, IT.8, IT.24). This is the result of the transformation of the IT department's role and the shift of power to the business departments, as surfaced from the data analysis. As noted by some participants (IT.8, IT.14, IT.17, IT.16), the role of the IT department is evolving from being prescriptive to being proactive. The digitalization of organizations, which emerged with CC, has emphasized the importance of putting the business departments first and being more oriented towards their needs. This is also supported by the co-construction witnessed in a few organizations, where the IT and business departments are working together and building projects together (IT.5, IT.13). Organizations that seem to be aware of the need for collaboration between the IT department and the business units tend to have a decentralized structure when making cloud decisions. This leads to a better understanding of business requirements and a better alignment between the choices of cloud services. In addition, our findings result in the presence of the federal archetype, which consists of multiple governing bodies working on different hierarchy levels (B.6, IT.3, IT.12, IT.14, IT.17, IT.18). And finally, the feudal archetype makes a small appearance, which consists of having each business unit making their own decisions in order to optimize their local needs (IT.11, IT.15, IT.16). Even though many archetypes emerge from the data analysis, several authors in the literature note that decision rights should be shared by the IT department and business departments with a greater ownership by one of the two. In addition, this decision-making process cannot occur without implementing governance mechanisms.

Governance mechanisms consist of decision-making structures, business processes, and relational mechanisms. Their aim is to work together in order to guide departments and encourage them to a specific organizational behavior (Weill and Ross 2004; De Haes and Van Grembergen 2009; Simonsson et al., 2010). Once organizations truly understand these objectives, they will be able to implement them to fulfil their intended purposes. In addition, when these governance mechanisms are taken in aggregate, they form the governance system in organizations. Nevertheless, the literature is not developed enough in addressing various cloud-related governance mechanisms. For instance, many researchers addressed the required decision-making structures that would facilitate the implementation of an effective IT governance. However, research work tackling structures specific to cloud computing is still scarce. Many structures were mentioned by our participants and are present in the literature, including IT steering committee, IT strategy committee, centers of competency, Chief Digital Officer, and having the CIO and CEO regularly report to the board. IT steering committees are agreed to be committees responsible for steering and monitoring IT and cloud-related projects. Their role is essential for the implementation of cloud services. Similarly, IT strategy committees are deployed to manage and control the evolution of the organization’s strategy with the adoption of cloud services. Centers of competency is agreed to be important in helping IT employees work together, share their skills and coordinate them. In addition, the dense presence of Chief Digital Officers (CDOs) in the literature as well in the data analysis emphasizes its importance today. The CDO's objective is to regroup the various departments and help them find solutions to the transformation issues the organization is facing. The CDO possesses business expertise while being digital savvy. This is what helps the organization in governing cloud-related decisions. Finally, the last common decision-making structure between the literature and participants is having the CIO and CEO report to the board. This governance structure appears to be important in order to promote communication and transparency throughout the organization. The rest of the structures cited by our participants were not specifically provided by researchers. The data analysis emphasizes the need of adopting structures devoted for cloud services, including an architecture board, a technical architecture committee, a chief data privacy officer, a digital project manager, a chief security officer, a purchasing committee, a legal technical committee, a chief exchange and digital officer, a data management committee, a scrum master, and data mining experts. While several organizations deployed common decision-making structures, some only focused on the mostly cited ones.

Moreover, the business processes are also not addressed enough by the literature and our participants. It appears that organizations are either not interested in building cloud-related governance processes, or they lack the competences to do so. The literature and the data analysis agree on the adoption of agile methodologies, governance frameworks, balanced scorecards adapted for cloud services. Through agile methodologies, organizations can benefit from the agility of their processes provided by cloud services. Governance frameworks can be useful to monitor the organizations' risks, for instance, when adopting cloud services. In addition, balanced scorecards help organizations align their business activities with their strategies, monitor their performance, and improve internal and external communication. While cloud services influence the organization's strategy, performance, and communication, it is important to deploy balanced scorecards. Few participants stated the implementation of specific governance processes. However, organizations are still not mature enough to adopt more business processes.

Finally, the literature along with the results from our analysis present several relational mechanisms mentioned by a large number of our participants, showing an advanced understanding in the need for such mechanisms. For instance, participants emphasize the closer relationship and regular communication between their business and IT departments, the presence of cross-functional job rotations and trainings within their organizations, raising cloud awareness through campaigns, ensuring a shared understanding of business and IT objectives, and a closer relationship with cloud service providers. While relational mechanisms are highly mentioned in the literature and our participants, they highlight the importance of communication, closer relationship, and understanding the different objectives.

Nevertheless, when comparing the different governance mechanisms implemented by our participants and the ones present in the academic literature, it shows that the latter is mostly scarce regarding decision-making structures and business processes. Hence, the suggested governance mechanisms by our participants represent an added-value to the scarce literature. Furthermore, as the data analysis showed the various set of governance mechanisms adopted by the participants' organizations, it highlights the number of mechanisms differing in cloud-related decision-making structures, business processes, and relational mechanisms (as illustrated in Figure 40). Figure 40 aims at emphasizing the lack of deploying cloud-related business processes and the various different choices of cloud-related decision-making structures. However, our participants agree on the implementation of cloud-related relational mechanisms.


**Figure 40: Summary of governance mechanisms adopted by participants**

Based on the stated cloud-related decisions, decision-making groups, and governance mechanisms, we can thus answer our research question "*Does the adoption of cloud services require a specific governance model*?" by affirming that cloud services do require a specific governance model. In addition, based on Figure 40, we can conclude that no organization has the exact similar governance model. While it is important to implement several governance mechanisms, their large number, for instance, leads to various possible governance models.

## II. Cloud Governance Models

After verifying that cloud services require a specific governance model, we decided to confirm it through exploring these organizations' cloud maturity (in other words, the intensity level of their cloud services adoption). Then, based on this approach we were able to study the various factors influencing their maturity and governance. Through 18 questions we evaluated the cloud maturity of each organization in 8 different domains; business strategy; organization and skills; governance; project, portfolio and services; architecture; operations; infrastructure; and information. This approach represents a self-assessment for organizations, while it allows them to position their domains maturity in one of the 5 proposed cloud maturity levels. In addition, the total cloud maturity average of each organization allowed their classification into 3 groups; organizations having a defined and systematic cloud maturity (CMM3), an opportunistic cloud maturity (CMM2) or simply an Ad Hoc cloud maturity (CMM1). In order to verify the pertinence of this classification, we compared the characteristics of each group to the definition of each cloud maturity level, provided by the ODCA (2013). Organizations possessing a CMM3 cloud maturity level introduced governance mechanisms and risk tools, which helped them reach this level of maturity. While organizations of group 2 (CMM2) have all embraced their private clouds, the cloud computing approach has not yet been widely accepted throughout their departments. Finally, organizations of the last group (CMM1) are still operated under their traditional IT processes, lack automation and have only deployed basic SaaS cloud solutions. Therefore, when compared to the Cloud Maturity Model levels presented by the ODCA (2013), we can affirm that these organizations were classified in the appropriate groups.

Having three groups with different cloud maturity levels allowed us to compare them and conclude with key factors leading to these different maturity levels. Hence, based on the data analysis of both parts (I and II), we developed a cloud governance framework. As shown in our framework, governing cloud services is affected by the decisions made, the choice of the decision-makers, the locus of the organization’s IT governance, the governance mechanisms adopted, the corporate strategy and the education of employees. First of all, organizations need to address primordial cloud-related decisions before deploying any cloud service. Organizations need to redirect their focus and priorities on decisions that are related to the correct adoption of cloud services. As presented previously, numerous cloud-related decisions emerged from the data analysis; the choice of merging towards cloud computing under the question ‘Why Cloud?’, the required transition steps to take into consideration, the cloud deployment and service models to adopt, the various data storage options, the financial and security issues, the required skills to operate cloud services, the cloud contract contents, the technical transition guidance, the choice of cloud service providers, the policy options, and the relationship with their customers. However, making these decisions constitute a primordial step for organizations. Thus, the most appropriate decision-makers are responsible for these decisions. As mentioned previously, the data analysis highlights decisions made by the IT department solely, through collaboration between the different departments, or by different subsidiaries. It is very important to allocate the most suitable group with the right skills to make the most appropriate decisions. The locus of the IT governance also plays a key role in the governance of these solutions. For instance, governing cloud services in a centralized IT governance differs from a decentralized one. Furthermore, organizations need to adopt sufficient cloud governance mechanisms, including cloud-related decision-making structures, business processes, and relational mechanisms. They aim at helping in the decision-making process and the governance of cloud services. Moreover, the data analysis pinpoints the corporate strategy behind their choice of cloud services (competition, innovation, or reduction of costs). Finally, the education – developing skills and competences – is also necessary when dealing with cloud services. It is also important to notice that several contingency factors also influence the governance of cloud services.

Therefore, based on these results and on the presence of different contingency factors affecting the governance, different cloud governance models emerged. The four governance models shown in our Findings chapter highlight the average number of decisions addressed by these organizations, the decisions made through collaboration or solely the IT department, their decentralized/centralized IT governance, the average number of mechanisms adopted as well as the average skills level of their employees. The emergence of these models also answers our research question proving that cloud services require a specific governance model. For instance, organizations adopting the first governance model (Figure 36) are decentralized, their decisions are made through collaboration between the various departments (on average 5 cloud-related decisions), their average maturity skills is 2.8 over 5 (their skills improved from being operational to strategic), and they adopt on average 7 governance mechanisms. These specificities are different from one governance model to the other, as shown in Table 30. Furthermore, when analyzing the different domains of the 35 organizations, it appears that some are more developed than others. This was illustrated by the various spider charts. Through these charts, organizations can assess the capabilities they need to develop in order to increase a specific domain maturity level.

**Table 30: Governance models comparison**

| **Characteristics** | **Governance Model 1 (Figure 36)** | **Governance Model 2 (Figure 37)** | **Governance Model 3 (Figure 38)** | **Governance Model 4 (Figure 39)** |
|---|---|---|---|---|

| **Cloud Maturity Model Level** | CMM3 | CMM2 | CMM2 | CMM1 |
|---|---|---|---|---|
| **Locus** | Decentralized | Decentralized | Centralized | Centralized |
| **Decision Makers** | Collaboration | Collaboration | IT department | IT department |
| **Avg. number of cloud-related decisions** | 5 | 3 | 2 | 2 |
| **Avg. skills maturity** | 2.8 | 1.9 | 1.6 | 1.0 |
| **Avg. number of governance mechanisms** | 7 | 3 | 2 | 1 |

As shown previously, four different governance models emerge from the data analysis with respect to the organizations' intensity level of the adoption of cloud services. This confirms again our research question, stating that cloud services need specific governance models.

Organizations adopting the same governance model have similar behavior in governing cloud services. They also work on almost the same domains. For instance, organizations adopting the first governance model (Governance model for Group 1 – CMM3) have the highest intensity level of their adoption of cloud services. In addition, these organizations focus on risk management and on developing their security capabilities in order to learn how to face risks. Moreover, they developed formal cloud trainings for their employees. Offering trainings is a primordial step to coach employees how to deploy cloud services, where new skills and competences are required. These organizations also pay a lot of attention, on the one hand, to the compliance of the providers when dealing with sensitive data stored on public clouds, and on the other hand on implementing governance mechanisms that would work together and guide them through the desired organizational behaviors. Finally, the deployment of an enterprise strategy positioning the use of cloud services and an adoption framework are similar characteristics of these organizations. Organizations based on the second governance model (Figure 37) possess a CMM2 intensity level of adoption of cloud services. Similarly, these organizations are also aware of the risks generated by cloud services. They, thus, implemented risk management throughout the organizations while updating their security skills. While some of these organizations updated their architecture processes and some developed their infrastructures, only a few have adapted their structures to cloud computing. In addition, these organizations have updated their strategies in order to be adapted to cloud services. Nevertheless, organizations based on the third governance model (Figure 38) do not differ a lot from the previous ones. Their centralized nature pushed them to implement risk management and update their security skills, as well as their organization's strategy. Finally, organizations governing their cloud services according to the last governance model presented (Figure 39) are only interested in managing the possible risks and their security skills. These organizations are controlled by the IT department making all of the decisions. They have adopted a low intensity level of cloud services. This links back to the large set of threats mentioned by the participants from these organizations.

The four governance models depend on the different cloud maturity of organizations (their intensity in adopting cloud services). As portrayed in the academic literature, the organization's maturity is identified as a contingency factor having an impact on its IT governance (Brown and Grant, 2005). The literature also pinpoints other contingency factors that affect organizations' IT governance, including the firm size, the geographical location, the sector, the industry, the corporate governance structure, the governance experience, the economies of scope, the corporate strategy and the organizational maturity (Starre and de Jong, 1998; De Haes & Van Grembergen, 2006; Ahituv et al., 1989; Brown and Magill, 1994; Clark, 1992; Tavakolian, 1989; Weill, 2004; Sambamurthy and Zmud, 1999, Brown and Grant, 2005). Based on the results from Part I and II, we can identify the following contingency factors affecting the governance of cloud services (as shown in Figure 41): the sector (private and public organizations), the industry (various industry types), the corporate strategy (cost, innovation, and competition focused), the IT governance type (centralized and decentralized) and the cloud adoption maturity (CMM1, CMM2 and CMM3). While the firm size (large organizations) and geographical location (France) are fixed factors, we cannot consider them as contingency factors in the case of our analysis. It is also important to note that due to the fixed geographical location (France), the education system as well as the syndicates are also fixed factors in our data analysis. For instance, employees in French organizations possess a French mentality and culture, they have mostly attended a French education system, and they possess the same syndicate groups. According to our analysis the education system and the syndicates have an impact on the cloud adoption maturity. However, the fact that these factors are fixed in our analysis represents a limitation for our research work.

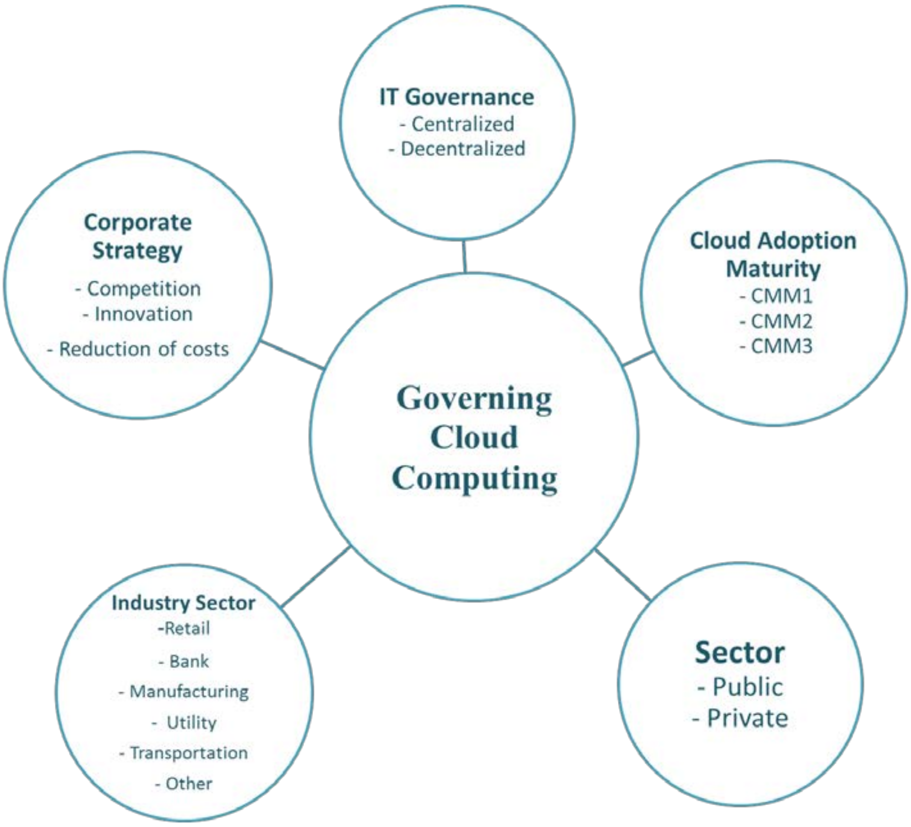


**Figure 41: Contingency factors for governing cloud services (source: participants)**

## III. Limitations

Based on the data analysis of Part I and II, we built a cloud governance framework representing several factors impacting IT governance. Decisions, decision-makers, governance mechanisms, employees' educations, and the corporate strategies emerged as impacting factors. Each factor contributes to the organization's IT governance in a balanced and propositioned manner. No factor bears more weight or contributes higher influence than another. Therefore, while we attributed the same weight to all the factors, our analysis might look limited. Some factors might contribute greater influence than others. Thus, this limitation pushes future research to look for ways to adjust this cloud governance framework where weights are attributed accordingly.

Additionally, through our data analysis, we were able to confirm the presence of a relationship between the IT governance of organizations adopting cloud services and their adoption intensity level. Even though no statistical study has been achieved, a correlation exists between IT governance and cloud maturity, based on the data analysis. However, no causal relationship has been proven in this research work, as this type of relationship requires a longitudinal study. This is where a major limitation of our research work stands. Between these two events, we could not prove that the occurrence of one causes the other. We do not have enough evidence to state first, that implementing an effective IT governance would cause a higher cloud maturity for the organization, and second, that having a high cloud maturity causes a more effective IT governance. The first step of this research work proved the presence of a correlation between these two elements. The following step would be investigating whether one action causes the other. Therefore, in order to explore the possible causality between the governance and the maturity, a longitudinal study can be achieved during future research.

The data analysis represented shadow IT practices under various aspects. We explored the reasons behind the presence of shadow IT in most of the 35 organizations, the cloud service models that are mostly concerned, and finally the impact of such practices on these organizations. We discovered that for some, shadow IT does not happen due to IT controls or collaborations between the IT department and business units. We can interpret this as a link to the centralization of their IT governance. Conversely, we noticed that due to departments' needs, the shift in power from the IT department to business units, and even with some assistance from the IT department, business units short-circuit it and seek solutions from cloud service providers. Nevertheless, we did not explore the correlation between the presence of shadow IT activities in an organization and its intensity level of its cloud adoption. We should be asking organizations whether these activities would decrease if they adopted more cloud solutions. It seems like this indirectly proportional correlation might exist. We surmise that if organizations adopted more (sophisticated) cloud services, especially ones required by the business departments, the latter will not need to bypass the IT department. This can also save organizations from risks generated by the recklessness of business units and their ignorance regarding the various security issues engendered from untrusty providers. In addition, when bypassing the IT department, business units do not pay attention to the signed contracts. Therefore, this can be considered as a limitation of our research work. A more in-depth study, thus, should be conducted with the same organizations. This study would address, in details, the different shadow IT practices the organizations are witnessing, the regularity of such practices, whether it would have been avoided if these services were internally implemented, and finally, whether the IT department would change their strategy in order to allow more services to be bought. As these interviews would be semi-structured, more questions would be addressed throughout the interview.

Furthermore, the education system and the education of syndicates emerged as important factors influencing the adoption of cloud computing from Part I. However, no academic literature exists to support our findings. The education system is linked to the students' trainings. However, the literature only addresses the need for professional trainings at work in order to deal with cloud technologies. Trainings should not only be implemented at work. They should start at school, where general classes (about the digital era, digital transformations, digital markets, etc.) should be offered. This will prepare graduate students in tackling the professional world with useful knowledge as their support. Thus, we believe that updated knowledge for graduate student as they start their professional lives can play an important role for their future organizations. Similarly for syndicates, the academic literature does not address their impacts on the organizations' intensity level of cloud adoption. Syndicates seem to be inhibiting organizations from adopting cloud services under the pretext that cloud computing is replacing some employees' jobs. Thus, educating syndicates and pushing them to become more open-minded and accepting of the digital transformation would be helpful for the growth of organizations. The limitation of our research work lies in proving the need of an updated education system and the education of syndicates. While this work builds on French organizations only, a similar education system and common syndicates binds the interviewed organizations. Therefore, future research needs to investigate the impact of the country's education system on the organizations' maturity (in cloud computing), and the impact of educating syndicates and having them on board during the adoption of cloud services.

## IV. Future Research

Based on the previously cited limitations of our research work, several opportunities for future research exist.

A first future research work would be to test our theoretical cloud governance framework in different organizations. This can be viewed as a first step for building a model that has been tested and improved accordingly, aiming at governing cloud services.

Furthermore, a longitudinal study can be interesting in order to explore the possible causal relationship between the organization’s IT governance and its intensity level of adopting cloud services. This causality helps organizations to elaborate the cause and effect relationship between their governance and their intensity level of adoption.

Additionally, a comparative analysis between “agile” and “traditional” organizations would bring insights on how cloud computing affects the organizational context and is affected by it. This comparative research study can be also beneficial on the change management level. For instance, conducting in-depth interviews with stakeholders involved in different environments (agile and traditional environment) help in identifying “best practices” that organizations need to implement when adopting cloud services.

Moreover, an in-depth study would be conducted regarding shadow IT practices. Future research would explore the possible correlation between the intensity level of shadow IT activities and the adoption of cloud services. With the presence of a correlation from this research work, the research study could reveal ways to decrease shadow IT practices in organizations.

Last but not least, studying the allocation of different weights to the factors of our cloud governance framework is important. It is an added-value as it reveals which factor has a higher impact on the organization’s governance and cloud adoption. Then, organizations can use these results in deploying the appropriate factors that will enhance the effectiveness of their IT governance and increase the intensity level of the adoption of cloud services. Thus, organizations can focus on certain factors in particular.

# V. Novelty of Research

## 1. Theoretical Implications

After two rounds of interviews, the data analysis highlighted several factors influencing organizations when adopting cloud services. While only a few of these factors are evoked by researchers, our findings add new knowledge to the academic literature. For instance, it highlights the transformations affecting the role of the IT department; its power is shifting towards business units during the cloud computing era. Our research work also pinpoints the emergence of a co-construction between the different departments during the development of a required IT service. In addition, the data analysis accentuates the importance of developing adapted skills to monitor cloud services. Even though the need for skills adapted for cloud computing is mentioned in the academic literature, our data analysis highlights its important influence on cloud adoption. The need to update the country's education system and train syndicates also emerge as critical factors influencing the intensity level of cloud adoption.

Our research work contributes to the academic level with the emergence of a new theoretical cloud governance model. The latter pinpoints new decision-making structures, business processes, and relational mechanisms identified by our data analysis. The academic literature remains scarce regarding the governance mechanisms adapted to the implementation of cloud services. While the literature does not address the main decisions to consider when adopting cloud services, our findings highlight different important categories to take into consideration before shifting to cloud computing. The governance model also emphasizes the importance of the locus of decisions along with the decision makers. As mentioned earlier, power is shifting from the IT department to the business units with the presence of cloud services. This means that business units must be part of the decision making process when dealing with cloud decisions. Their input is as important as the IT department's. Therefore, the complete set of mechanisms, cloud-related decisions, and decision makers identified in our data analysis would serve as an added-value to the academic literature. Additionally, from the set of factors identified in our data analysis and influencing the governance framework, the education of all employees is also an added-value to the academic literature. Finally, through our cloud governance framework, a correlation between the cloud governance of organizations and their intensity level of cloud adoption was identified. It is important to take into account this correlation as it motivates organizations to adopt a better and more effective IT governance while it is linked to their cloud adoption intensity levels. Nevertheless, as mentioned in our future research section, we aim at further testing this governance framework in order to validate its effectiveness with more organizations from different countries.

## 2. Practical Implications

Organizations seeking to adopt cloud services need to be aware of the different transformations that have to be taken into consideration before their transition. Organizations should address the various impacts of cloud computing. Based on the previously cited cloud-related decisions and on the choice of the most appropriate decision makers, organizations can study their transition through discussions and collaboration between the different departments. In addition, as more collaboration and synergy emerge in organizations, they can take into account the various cited impacts in order to improve their governance and increase their cloud adoption. For instance, they can start by investing in training programs for their employees, whether internally or through external platforms. As the IT department role is slowly but surely shifting, organizations need to be aware of the right transitions in order to accommodate this shift. Furthermore, through collaboration and more discussion with the IT department, organizations can deploy new secure cloud services and hence, fight generated risks and shadow IT practices. In addition, organizations can base their analyses and decisions on the proposed cloud governance framework in order to improve their governance and hence increase their cloud adoption intensity levels.

# Conclusion

As you have made it this far, this chapter will be a recapitulation of what you have read throughout this manuscript. The conclusion chapter aims at highlighting the important concepts addressed in our research work and underlying the answer to our research question. Moreover, we will elucidate the specificity of the contribution to the cloud computing literature, while stressing on the usefulness and impact of our research. Finally, we will end this chapter with a reminder of possible future research. .

The emergence of new technologies, particularly cloud computing, is the proof that the Internet has been reshaping today's society. People's needs have been evolving, increasing and changing in a very short time lapse. This is occurring due to the myriad of services available for users, and offered by cloud service providers. The promising cloud computing market is leading to an increased number of organizations migrating to a public, private, hybrid or communal cloud environment. According to a forecast by Gartner (2016), the number of organizations not adopting cloud services in 2020 will be equal to the number of organizations not using the Internet today. This emphasizes the high and fast expansion of cloud technologies across society, markets, and organizations. The five characteristics of cloud computing allow its fast expansion; on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. According to an exhaustive literature review and to our findings, a long list of benefits makes cloud computing appealing to organizations. It first offers economic benefits. For instance, cloud services provide economies of scale for providers, low prices for users due to the pay-per-use characteristic, a shift from capital expenditures (CAPEX) to operational expenditures (OPEX), lower electricity consumptions, easy market entrance for start-ups, SMEs, and developing countries. In addition, the scalability offered by cloud services is highly attractive, where users have the possibility to possess computing resources on demand as well as scale up and down dynamically through a minimal interaction with their cloud service providers. Furthermore, along with the good quality of services, simplified operations and robust machines provided by cloud services, they also offer new applications and services, new markets, as well as low IT barriers to innovation. Besides, organizations are presented with more agile processes, a lower time-to-market, an easy access to services and optimized resource utilization. Finally, the ubiquitous access of data and services seems to be a highly attractive characteristic of cloud computing.

Nevertheless, the adoption of cloud services is still not fully expanded as they generate numerous risks, according to an exhaustive literature and our findings. Organizations rate cloud security as major issues, where the confidentiality and sensitivity of their data are highly important. In addition, organizations are anxious about insider and outsider attacks along with the possibility of losing their data in a public cloud environment. Moreover, due to several regulations and integrity laws, as well as the location of critical data, organizations do not feel safe storing their data with cloud service providers outside of their own countries.

Numerous other risks are generated including the culture resistance to change, integrating new applications to the organization's IS, the unsuitability of migrating existing applications to the cloud infrastructures and platforms, the limited customization that affects the organization's competitiveness, the availability of servers, and the possibility of offers from untrusted providers. In addition, organizations are skeptical due to the presence of congestion, unpredictability, bugs in large distributed systems, downtime, poor broadband connectivity, and bottlenecks. Furthermore, with the emergence of cloud services, organizational witness contractual and technical reversibility as well as a lack of competences and trainings.

Therefore, even with the large set of benefits achieved through the adoption of cloud services, organizations are far from fully transitioning to the cloud due to the dominance of critical and risky challenges. In addition, organizations have been going through different transformations due to the emergence of cloud services.

Cloud computing has been transforming organizations in various ways, starting with the IT department. While the latter was a primordial element when dealing with IT services, its role has been changing with the emergence of cloud technology. Previously, the IT department aimed at delivering services within budget and time. Today, its aim has shifted towards being focused on the business departments while using IT in achieving business needs. As business employees are highly reactive to the market, they are continuously seeking ways to innovate and impact it. In addition, the digital transformation is influencing the role and position of the IT department within the organization. For instance, business departments act independently as they are being contacted by cloud service providers. They do not require the IT department's assistance for developing new services, which can constitute a risk in the organization. With the shift of sovereignty and power, the IT department is pressured into changing its strategy from being prescriptive to proactive. Therefore, the emergence of cloud services is transforming the dynamics within organizations.

Along with the transformations witnessed within the organization, the emergence of cloud services impacts it in several ways. First, employees, especially in the IT department, are pushed to develop their skills in order to be capable of dealing with cloud services. For instance, the role of the CIO in organizations is constantly evolving in order to adapt to the changing business needs. CIOs should not only keep their IT knowledge, but they should also develop some business knowledge as well. This emphasizes the involvement of the CIOs in the IT and business sides of the organization. In addition, while the IT department is no longer considered just a service supplier, it should be part of the business arbitration. Furthermore, it is important to note that the adoption of cloud solutions is also changing the hiring criteria of IT people as well as the training program content. Therefore, universities must adapt their teaching methodologies and programs to fit the digital era, from its different aspects and regarding its numerous concepts. Moreover, according to our findings, syndicates need to be on board with the organization’s choices, to avoid inhibiting their cloud adoption process. Thus, these syndicates need to be educated about the benefits gained through cloud adoption. This represents highly important impacts of cloud technology on today’s organizations, market, and society.

Furthermore, cloud computing has been influencing organizations’ processes and infrastructures. For instance, organizations have been structuring their processes into more automated and agile ones, through breaking their traditional organizational models. According to our findings, they have been witnessing shorter development cycles, more communication between their departments, and faster developed services by the IT departments that are better answering their business departments’ needs. In addition, with the presence of numerous IaaS offers, organizations are also questioning whether to develop internal applications or to simply adopt public cloud services. This emphasizes the impact of such services on organizations’ processes and infrastructures.

Along with the appearance of cloud computing, the concepts of data privacy and contractual security have emerged. While security teams used to monitor their organization’s security through conducting various security tests, today, they need to ensure the reliability of cloud contracts agreed upon with the organization’s cloud service providers. They should monitor that the proposed contracts cover the required standards regarding the cloud solutions security. Therefore, this impact leads to the need of developing new competences in understanding and meticulously reading cloud contracts. *De facto*, security is a high issue for organizations adopting cloud services, as their data is considered as one of the most important assets. While they realized that their data possess a sacred value, they need to closely monitor their cloud services security.

Furthermore, implementing cloud services impacts organizations as they create a strong link with their cloud service providers. This relationship is primordial as providers are part of the cloud computing ecosystem. Therefore, keeping a transparent, trusting, and respectful relationship would be beneficial for both parties.

Another influence of cloud computing is the increased shadow IT activities in organizations. Business departments short-circuit their IT department when their needs are not properly fulfilled. The moment these departments realize that their IT teams do not possess the appropriate services to accomplish their projects, they tend to get frustrated and contact cloud services providers to buy external solutions. Through cloud computing, business departments possess more freedom to contract with providers when they need to. This sheds the light on the previously discussed transformations generated by cloud services, where the IT department is losing its control and power over IT. However, this also links to the risks associated with cloud computing. For instance, business departments are unaware of certain legislation issues where some countries do not permit their data to be stored outside of their territories. Thus, as they adopt services from cloud service providers without being aware of the compliance state, they get their organization into serious issues.

While cloud technology engenders numerous transformations in the organization and impacts it in several different ways, it also generates various internal and external risks. Consequently, in order to avoid these risks while benefiting from the promised advantages, organizations are faced with the need for effective governance. It is important to remind that governance is primordial for the survival of organizations, as it helps them achieve their business objectives. Through cloud governance, organizations are capable of monitoring, controlling and administering their cloud adoption process as well as their cloud service usages. Organizations will also be able to make the most appropriate choices regarding their cloud adoption and fittingly implement these choices. Nevertheless, as discussed throughout this research work, the literature addressing cloud governance in organizations is still scarce. No effective cloud governance tackling it as a whole and from different angles exists to our knowledge. However, as cloud computing is considered as a part of the organization’s IT, the aim of this research was to see whether cloud services can be governed through the actual organization’s IT governance.

We based our work on the definition of IT governance proposed by Luftman and Brier (1999), Sambamurthy and Zmud (2000), Peterson (2004), and Weill (2004). These authors suggest that an organization’s IT is governed through appropriate decisions, decisions makers, and governance mechanisms. After two rounds of interviews, and using this IT governance definition, findings emphasized that cloud computing needs specific IT governance models, which answers our research question. In fact, traditional IT governance does not cover the new cloud-related decisions, does not take into account the new dynamics between stakeholders, and does not provide the required governance mechanisms in order to deploy effectively cloud services within the organization.

Based on our data analysis, we developed a cloud governance framework that illustrates the different factors impacting the governance of cloud services through the organization's IT governance. For instance, in order to govern cloud services, the organization needs to address cloud-related decisions. While such decisions are not highly mentioned in the academic literature, we identified critical ones through the analysis of our results. For instance, organizations need to address decisions regarding the motivation to move to the cloud, the required organizational and technical transition steps, the needed deployment and service models, the data storage options, the financial and security issues, the required skills and competences, the cloud contract content, the cloud service providers choice, the policy requirements, and finally the relationship with their customers. Along with the cloud-related decisions, the organization should allocate them to the most adequate decision-makers. Our findings highlighted the link between the governance locus and the decision-makers. As the emergence of cloud services in organizations changes the dynamics between the different stakeholders, the decision-making process differs from the traditional one; new stakeholders are involved in this process. For instance, while decisions in centralized organizations are made by the IT department, they are made through collaboration of different departments in decentralized organizations. Finally, in order for these decisions to be implemented, organizations need governance mechanisms that differ from ones found in the existing IT governance models. Our findings resulted in numerous cloud-related decision-making structures (CDO, center of competency, Chief Data Privacy Officer, Digital Project Manager, Scrum Master, etc.), business processes (governance frameworks, agile processes, balanced scorecards, etc.), and relational mechanisms (closer and more regular communication between departments, cross-functional business and IT job rotations and trainings, awareness campaigns, shared understanding between business and IT employees, etc.) All these mechanisms constitute an added-value for the cloud governance literature. Furthermore, from the developed cloud governance framework, a link between the organization's governance and the intensity level of the adoption of cloud services (i.e. cloud maturity) emerged. Several factors influencing the organization's cloud maturity were also identified. For example, the motivation behind adopting cloud services plays an important role in the intensity level of adoption. When competition pushes organizations towards cloud computing, these organizations are prone to increase their adoption in order to beat their competitors. Moreover, developing the required skills and competences for dealing with cloud services is critical for the intensity level of adoption. Similarly, adapting the country’s education system and having syndicates on board provide a higher probability for a higher intensity level of the country’s organizations.

Our cloud governance framework along with the second round of interviews led to the emergence of different cloud governance models depending on the cloud maturity of the organization. We identified 4 cloud governance models, one specific for a cloud maturity of CMM3, two for a cloud maturity of CMM2, and the last for a cloud maturity of CMM1. These models differ on the average number of cloud-related governance mechanisms adopted, the locus of decisions, the decision makers, the number of cloud-related decisions addressed, and the skills maturity of the organization’s employees. The emergence of these models reaffirms our research question; cloud services do need a specific governance model.

The adoption of cloud services has brought numerous changes and transformations in organizations. It has emphasized the need of changing the way IT projects are developed, managed and governed. Thus, new decision-making structures, relational mechanisms, development and management practices have emerged and been deployed throughout organizations. By promoting short development cycles, close collaboration between departments and continuous feedback, the technical and functional characteristics of cloud services has affected the organizational culture, structure, as well as the business processes and management principles. However, the adoption of cloud solutions has been also affected by the organization’s characteristics and stakeholders’ interpretations and perceptions. As our data analysis shows, contingency factors as well as stakeholders’ actions seem to affect the way cloud services are adopted and governed in large organizations. Hence, the cloud-related decisions, the decision-makers as well as the governance mechanisms can differ from one organizational context to another. Additionally, based on our findings, cloud computing is changing the dynamics of the organization. Therefore, its adoption is the product of stakeholders’ interactions and perceptions. In addition, it is important to note that the governance of cloud services can also be subject of stakeholders’ interactions and perceptions. From this perspective, cloud computing is being approached as shaping of, and shaped by, its organizational context (Orlikowski, 1992).

After discussing the various transformations and impacts of cloud services on organizations, it was shown that governing such services is not a simple task. In fact, large organizations will not be able to transition towards the cloud immediately. They should perform the switch gradually. Therefore, while basing their plans on the proposed cloud governance framework, organizations need to implement change management. This concept is an absolutely natural reaction to the altered situations that the organization goes through during the adoption of any technological innovation system and tool. Through change management, organizations can slowly bring changes to their employees through gradually informing them about the future changes and include them in the change process (for example, taking into consideration their needs and expectations, highlighting the benefits of adopting cloud services, and introducing them to the required trainings they need to assist, skills they need to develop, behavior they need to adapt, etc.). Along with the employees, organizations can bring changes to their infrastructures, processes, methodologies, etc. This is why implementing change management during the cloud adoption process represents a vital and required step for large organizations.

Furthermore, deploying a stakeholder analysis before implementing an effective cloud governance in the organization is a smart step in the change management process. Through the stakeholder analysis, organizations will be capable of identifying the key stakeholders involved in the cloud adoption process and analyze their contribution to the change management project. After identifying the primary stakeholders, this analysis allows organizations to explore their needs, perceptions, power, and influence. Then, organizations will be able to allocate the most appropriate decision to the adequate decision-makers. Hence, with the help of a stakeholder analysis, organizations will be one step further to effectively governing their cloud solutions.

Our research question was answered by the development of a cloud governance framework leading to the emergence of different cloud governance models. Therefore, our research work contributes to the academic literature through providing organizations with new methods to effectively govern their cloud services. It also contributes to the information system literature by highlighting the dual nature of cloud technologies in the way their adoption affects organizations and is affected by them.

Even though our research work provides several contributions to the literature, it remains limited. This provides us with opportunities for various future research ideas, as discussed earlier. First, it would be important to test our theoretical cloud governance framework as a first step for building a tested and improved model aiming at effectively governing cloud services. Then, in order to explore the possible causal relationship between the organization's IT governance and its intensity level of cloud services adoption, a longitudinal study would be required. In addition, conducting a comparative analysis between "agile" and "traditional" organizations would be beneficial on the change management level. Comparing stakeholders involved in different environments would identify "best practices", helpful for the cloud adoption process. Moreover, future research can explore the correlation between the intensity level of cloud adoption and the intensity of shadow IT activities within organizations. Finally, we identify as further studies, exploring the different weights allocated to the cloud governance framework factors. This study aims at revealing which factor possesses a higher influence on the organization's governance as well as on its cloud adoption.

# Bibliography


Adams, C. R., Larson, E. C., & Xia, W. (2008). IS/IT Governance Structure and Alignment: An Apparent Paradox. *Management Information Systems Research Center*. Retrieved from http://www.misrc.csom.umn.edu/workshops/2008/spring/Larson_Spring_08.pdf

Ahituv, N., Neumann, S., & Zviran, M. (1989). Factors Affecting the Policy for Distributing Computing Resources. *MIS Quarterly*, *13*(4), 389–401.

Ahuja, S., & Gallupe, B. (2015). A Foundation for the Study of Personal Cloud Computing in Organizations. *Proceedings of the 21st Americas Conference on Information Systems (AMCIS), Puerto Rico.*

Ali, S., & Green, P. (2012). Effective information technology (IT) governance mechanisms: An IT outsourcing perspective. *Information Systems Frontiers*, *14*(2), 179–193.

Alter, S. (2002). The work system method for understanding information systems and information systems research. *Communications of the Association for Information Systems*, *9*(1), 90–104.

Alter, S. (2014). Theory of Workarounds. *Communications of the ACM*, *34*(1), 1041–1066.

Applegate, L., Holsapple, C., Katakota, R., Radermacher, F., & Whinston, A. (1996). Electronic Commerce: Building Blocks of New Business Opportunity, *Journal of Organizational Computing and Electronic Commerce*, *6*(1), 1–10.

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50–58.

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.

Babcock, C. (2010). *Management Strategies for the Cloud Revolution: How cloud computing is transforming business and why you can't afford to be left behind*. New York: McGraw Hill Professional.

Bahli, B., & Rivard, S. (2005). Validating measures of information technology outsourcing risk factors. *Omega*, *33*(2), 175–187.

Bate, R., Kuhn, D., Wells, C., Armitage, J., Clark, G., Cusick, K., Garcia, S., Hanna, M., Jones, R., Malpass, P., et al. (1995). *A systems engineering capability maturity model Version 1.1* (CMU/SEI-95-MM-003). Pittsburgh: Carnegie Mellon Software Engineering Institute.

Battleson, D. A., West, B. C., Kim, J., Ramesh, B., & Robinson, P. S. (2016). Achieving dynamic capabilities with cloud computing: an empirical investigation. *European Journal of Information Systems, 25*(3), 209–230.

Beaudry, A., & Pinsonneault, A. (2005). Understanding user responses to information technology: A coping model of user adaptation. *MIS Quarterly*, 29(3), 493–524.

Behrens, S., & Sedera, W. (2004). Why do shadow systems exist after an ERP implementation? Lessons from a case study. *Proceedings of the 8th Pacific Asia Conference on Information Systems (PACIS)*, Shanghai, China.

Beimborn, D., Franke, J., Wagner, H.-T., & Weitzel, T. (2007). The impact of operational alignment on IT flexibility-Empirical evidence from a survey in the German banking industry. *Proceedings of the 13th Americas Conference on Information Systems (AMCIS)*, Colorado, USA.

Benbasat, I., Goldstein, D., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS quarterly*, *11*(3), 369–386.

Benlian, A., & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. *Decision Support Systems*, *52*(1), 232–246.

Bennett, C., & Timbrell, G. (2000). Application service providers: will they succeed?. *Information Systems Frontiers*, *2*(2), 195–211.

Benvenuto, N. A., & Brand, D. (2005). Outsourcing-A risk management perspective. *Information Systems Control Journal*, *5*, 35.

Bergeron, F., Raymond, L., & Rivard, S. (2004). Ideal patterns of strategic alignment and business performance. *Information & Management*, *41*(8), 1003–1020.

Bernstein, D., & Ludvigson, E. (2009, May). *Networking Challenges and Resultant Approaches for Large Scale Cloud Construction*. Paper presented at the 2009 Workshops of the Grid and Pervasive Computing Conference, Geneva, Switzerland.

Beyer, J. M., & Nino, D. (1999). Ethics and cultures in international business. *Journal of Management Inquiry*, *8*(3), 287–297.

Bhattacharjya, J., & Chang, V. (2006). Evolving IT governance practices for IT and business alignment: A case study in an Australian institution. *Proceedings of the Conference on Information Science, Technology and Management (CISTM 2006), Chandigarh, India*. Retrieved on the 14th of April, 2015 from https://espace.curtin.edu.au/handle/20.500.11937/42026

Bill, C., Heflleey-William, E., & Sally, M. (1995). *Overview of the People Capability Maturity Model* (CMU/SEI_95-MM-01). Pittsburgh: Carnegie Mellon Software Engineering Institute.

Bogdan, R. C., Biklen, S.K. (2003). *Qualitative for education: An introduction to theories and methods*. New York: Pearson Education Group.

Boudreau, M., & Robey, D. (2005). Enacting integrated information technology: A human agency perspective. *Organization Science*, *16*(1), 3–18.

Bowen, P., Cheung, M., & Rohde, F. (2007). Enhancing IT governance practices: A model and case study of an organization's efforts. *International Journal of Accounting Information Systems*, 8, 191–221.

Bowling, A. and Ebrahim, S. (Eds.) (2005). *Handbook of Health Research Methods: Investigation, Measurement and Analysis*. Maidenhead: Open University Press.

Boynton, A. & Zmud, R. (1987). Information Technology Planning in the 1990's: Directions for Practice and Research. *MIS Quarterly*, *1*(11), 58–72.

Boynton, A., Jacobs, G., & Zmud, R. (1992). Whose responsibility is IT management?. *MIT Sloan Management Review*, *33*(4), 32.

Bradshaw, S., Millard, C., & Walden, I. (2011). Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services. *International Journal of Law and Information Technology*, *19*(3), 187–223.

Broadbent, M. (2003). Understanding IT governance. *CIO Canada*, *11*(4), 13–14.

Broadbent, M., & Weill, P. (1991). *Developing business and information strategy alignment: a study in the banking industry*. Melbourne: University of Melbourne, Graduate School of Management.

Broadbent, M., & Weill, P. (1997). Management by maxim: how business and IT managers can create IT infrastructures. *MIT Sloan Management Review*, *38*(3), 77.

Broadbent, M., & Weill, P. (1998). Leading Governance, Business and IT Processes: the Organizational fabric of business and IT partnership. *Gartner ITEP Findings*.

Broom, A., Cheshire, L., & Emmison, M. (2009). Qualitative researchers' understandings of their practice and the implications for data archiving and sharing. *Sociology*, *43*(6), 1163–1180.

Brousell, L. (2011, June 14). *Survey: CIOs are putting the cloud first*. Retrieved on the 16th June, 2015 from http://www.cio.com/article/684338/Survey_CIOs_Are_Putting_the_Cloud_First

Brown, A. E., & Grant, G. G. (2005). Framing the frameworks: A review of IT governance research. *Communications of the Association for Information Systems*, *15*(1), 38.

Brown, B. (2013). *IT budgets, salaries & priorities: 2013 SIM IT trends study*. Retrieved on the 18th of March, 2017 from https://www.networkworld.com/article/2289546/infrastructure-management/128060-IT-budgets-salaries-and-priorities-2013-SIM-IT-Trends-Study.html.

Brown, C. (1997). Examining the Emergence of Hybrid IS governance Solutions: Evidence from a Single Case Site. *Information Systems Research*, *8*(1), 69–95.

Brown, C. (1999). Horizontal mechanisms under differing IS organization contexts. *MIS Quarterly*, *23*(3), 421–454.

Brown, C., & Magill, S. L. (1994). Alignment of the IS Functions with the Enterprise: Toward a Model of Antecedents. *MIS Quarterly*, *18*(4), 371.

Bruce, K. (1998). Can you align IT with business strategy?. *Strategy & Leadership*, *26*(5), 16–20.

Bryman, A., & Bell, E. (2015). *Business research methods*. New York: Oxford University Press Inc.

Brynjolfsson, E., Hofmann, P., & Jordan, J. (2010). Cloud computing and electricity: beyond the utility model. *Communications of the ACM*, *53*(5), 32.

Buchwald, A., & Urbach, N. (2012, December). Exploring the role of un-enacted projects in IT project portfolio management. *Proceedings of the 33rd International Conference on Information Systems (ICIS),* Orlando, USA.

Buckby, S., Best, P., & Stewart, J. (2008). The current state of information technology governance literature. *Information Science Reference (IGI Global).*

Buenstorf, G., & Fornahl, D. (2009). B2C—bubble to cluster: the dot-com boom, spin-off entrepreneurship, and regional agglomeration. *Journal of Evolutionary Economics*, *19*(3), 349–378.

Bunker, G., & Thomson, D. (2006). *Delivering utility computing: Business-driven IT optimization*. Hoboken, NJ: John Wiley & Sons Inc.

Burn, J. M., & Szeto, C. (1999). Effective Management of Information Technology-Closing the Strategic Divide!. *Journal of Scientific and Industrial Research,58,* 171–180.

Bussen, W., & Myers, M. (1997). Executive information system failure: A New Zealand case study. *Journal of Information Management*, *12*, 145–153.

Buyya, R., Yeo, C. S., & Venugopal, S. (2008, September). Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. *Proceeding of the 10th IEEE International Conference on High Performance Computing and Communications,* Dalian, China

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, *25*(6), 599–616.

Cafaro, M., & Aloisio, G. (2011). Grids, clouds, and virtualization. In M. Cafaro & G. Aloisio (Eds.), *Grids, clouds, and virtualization* (pp. 1-21). London: Springer.

Callahan, J., Bastos, C., & Keyes, D. (2004). The evolution of IT Governance at NB Power. In W. Van Grimbergen (Ed.), *Strategies for information technology governance* (pp. 343-356). United Kingdom: Idea Group Publishing.

Carr, N. (2008). *The Big Switch: Rewiring the world, from Edison to Google*. New York: W.W. Norton & Company.

Carr, N. G. (2003). IT doesn't matter. *Educause Review*, *38*, 24–38.

Carr, N. G. (2005). The end of corporate computing. *MIT Sloan Management Review*, *46*(3), 67.

CDO Club (2015). *3rd Annual NYC Chief Digital Officer Summit*. Retrieved on the 4th of March, 2016 from http://cdoclub.com/?wlfrom=%2Fnyc-2015%2F.

CDO Talent Map 2013 (2014). *CDO Club.* Retrieved on the 9th of June, 2016 from http://cdoclub.com/publications/.

Cerpa, N., & Verner, J. M. (1998). Case Study: The Effect of IS Maturity on Information Systems Strategic Planning. *Information & Management*, *34*(4), 199–208.

Chandler, D., & Munday, R. (2012). *A dictionary of social media (first Ed.)*. New York: Oxford University Press Inc.

Chapin, D. A., & Akridge, S. (2005). How can security be measured. *Information Systems Control Journal*, *2*(1), 1–6.

Charreaux G. (1997). Vers une théorie du gouvernement des entreprises. In G. Charreaux (Ed.), *Le Gouvernement des entreprises : Corporate Governance, théories et faits* (pp. 421–469). Paris : Économica.

Chatterjee, D., Grewal, R., Sambamurthy, V. (2002). Shaping up for e-commerce: Institutional enablers of the organizational assimilation of Web technologies. *MIS Quarterly, 26*(2), 65–89.

Chebrolu, S. (2011). Assessing the relationships among cloud adoption, strategic alignment and IT effectiveness. *Journal of Information Technology Management*, *22*(2), 13–29.

Chen, D., Preston, D., & Xia, W. (2010). Antecedents and Effects of CIO Supply-side and Demand-side Leadership: A Staged Maturity Model. *Journal of Management Information Systems*, *27*(1), 231–272.

Chua, W. (1986). Radical developments in accounting thought. *Accounting review*, *61*(4), 601–632.

Clark Jr, T. D. (1992). Corporate systems management: an overview and research perspective. *Communications of the ACM*, *35*(2), 61–75.

Cognizant. (2013). *Cognizant Announces Record Results For Second Quarter 2013*. Retrieved on the 17th of June, 2016 from: http://investors.cognizant.com/2013-08-06-Cognizant-Announces-Record-Results-For-Second-Quarter-2013

Collis, J., & Hussey, R. (2013). *Business research: A practical guide for undergraduate and postgraduate students*. Hampshire, United Kingdom: Palgrave Macmillan Press.

Conway, G., & Curry, E. (2012). Managing Cloud Computing: A Life Cycle Approach. *Proceedings of the 2nd International Conference on Cloud Computing and Services Science (CLOSER 2012)*, Porto, Portugal.

Cooper, J., & Fisher, M. (2002). *Software Acquisition Capability Maturity Model® (SA-CMM®) Version 1.03* (CMU/SEI-2002-TR-010). Pittsburg: Carnegie Mellon Software Engineering Institute.

Cornford, T., & Smithson, S. (2006). *Project research in information systems: a student's guide*. Hampshire, United Kingdom: Palgrave Macmillan Press.

COSO. (2004). *Enterprise Risk Management – Integrated Framework (1st Ed.)* Retrieved on the 5th of March, 2015 from https://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf.

COSO. (2012). *Enterprise Risk Management for Cloud Computing*. Retrieved on the 8th of March, 2015 from https://www.coso.org/Documents/Cloud-Computing-Thought-Paper.pdf.

Crawford, J. K. (2007). *Project management maturity model*. New York: Auerbach Publications.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*. London: Sage publications.

Croteau, A.M., & Bergeron, F. (2009). Interorganizational governance of information technology. *Proceedings of the 42nd Hawaii International Conference on System Sciences (HICSS),* Hawaii.

CSC Index (1998). *Critical Issues of Information Systems Management of 1998*. Cambridge: CSC (pp. 14–15).

Cumps, B., Viaene, S., Dedene, G., & Vandenbulcke, J. (2006). An empirical study on business/ICT alignment in European organisations. *Proceedings of the 39th Annual Hawaii International Conference on Systems Sciences,* Hawaii.

Damianides, M. (2005). Sarbanes-Oxley and IT governance: New guidance on IT control and compliance. *Information Systems Management*, *22*(1), 77–85.

Davenport, J. H., Siret, Y., & Tournier, É. (1988). *Computer algebra*. London: Academic Press.

Davern, M. J., & Kauffman, R. J. (2000). Discovering potential and realizing value from information technology investments. *Journal of Management Information Systems*, *16*(4), 121–143.

De Haes, S., & Van Grembergen, W. (2004). IT governance and its mechanisms. *Information Systems Control Journal*, *1*, 27–33.

De Haes, S., & Van Grembergen, W. (2005). IT governance structures, processes and relational mechanisms: Achieving IT/business alignment in a major Belgian financial group. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05),* Hawaii.

De Haes, S., & Van Grembergen, W. (2006). Information technology governance best practices in Belgian organisations. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, Hawaii.

De Haes, S., & Van Grembergen, W. (2008). Analysing the relationship between IT governance and business/IT alignment maturity. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences*, Hawaii.

De Haes, S., & Van Grembergen, W. (2009). An Exploratory Study into IT Governance Implementations and its Impact on Business/IT Alignment. *Information Systems Management*, *26*(2), 123–137.

Dillon, T., Wu, C., & Chang, E. (2010). Cloud computing: issues and challenges. *Proceeding of the 24th International Conference on Advanced Information Networking and Applications (AINA)*, Perth, Australia.

Dittes, S., Urbach, N., Ahlemann, F., Smolnik, S., & Müller, T. (2015). Why don't you stick to them? Understanding factors influencing and counter-measures to combat deviant behavior towards organizational IT standards. *Proceedings of the Multikonferenz Wirtschaftsinformatik*.

Dorfman, M., & Thayer, R. H. (Eds.). (1997). *Software requirements engineering*. Los Alamitos: IEEE Computer Society Press.

Duarte, A., & Da Silva, M. (2013). Cloud Maturity Model. *Proceedings of the Sixth International Conference on Cloud Computing*.

Duffy, J. (2002). *IT/Business alignment: Is it an option or is it mandatory (IDC document #26831)*.

Dumas, M., Van der Aalst, W. M., & Ter Hofstede, A. H. (2005). *Process-aware information systems: bridging people and software through process technology*. Hoboken, NJ: John Wiley & Sons.

Durkee, D. (2010). Why Cloud Computing Will Never Be Free. *Communications of the ACM*, *53*(5), 62–69.

Dutta, A., Peng, G. C. A., & Choudhary, A. (2013). Risks in enterprise cloud computing: the perspective of IT experts. *Journal of Computer Information Systems*, *53*(4), 39–48.

Earl, M. J. (1993). Experiences in Strategic Information Systems Planning. *MIS Quarterly*, *17*(1), 1–24.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of management review*, *14*(1), 57–74.

Elliott, R. and Timulak, L. (2005). Descriptive and interpretive approaches to qualitative research. In AUTHORS *Handbook of Resolved Methods for Clinical and Health Psychology*, (pp. 147–159).

Enns, H. G., Murray, E. J., & Huff, S. L. (1997). Shared understanding between IS and business executives: impacts on IS effectiveness and business performance. *Administrative Sciences Association of Canada-Annual Conference*, 18, (pp. 12–23).

Fama, E. F., & Jensen, M. C. (1983). Separation of ownership and control. *The Journal of Law and Economics*, *26*(2), 301–325.

Feeny, D. F., & Willcocks, L. P. (1998). Core IS capabilities for exploiting information technology. *Sloan Management Review*, *39*(3), 9–21.

Fielding, N. & Lee, R. (1991). *Using Computers in Qualitative Research*. London: Sage.

Fitzgerald, B., & Howcroft, D. (1998). Competing dichotomies in IS research and possible strategies for resolution. *Proceedings of the 19th International Conference on Information Systems*, Helsinki, Finland.

Fitzgerald, M., Kruschwitz, N., Bonnet, D., & Welch, M. (2013). Embracing Digital Technology. *MIT Sloan Management Review*.

Flechaux, R. (2009). *Cloud Computing : un DSI européen sur deux n'y connaît rien*. Retrieved on the 12th of June 2016 from http://www.lemagit.fr/actualites/2240196386/Cloud-Computing-un-DSI-europeen-sur-deux-ny-connait-rien.

Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008). *Cloud computing and grid computing 360-degree compared*. Paper presented at the *Grid Computing Environments Workshop*, Austin, Texas.

Freshwater, D., & Cahill, J. (2013). Paradigms lost and paradigms regained. *Journal of Mixed Methods Research*, *7*(1), 3–5.

Fürstenau, D., & Rothe, H. (2014). Shadow IT Systems: Discerning the Good and the Evil. *Proceedings of the 22nd European Conference on Information Systems (ECIS)*, Tel Aviv, Israel.

Galliers, R.D. & Leidner, D.E. (2003). *Strategic Information Management: Challenges and Strategies in Managing Information System*. Massachusetts: Elsevier Butterworth-Heinemann.

Garcia Reyes, H., & Giachetti, R. (2010). Using experts to develop a supply chain maturity model in Mexico. *Supply Chain Management: An International Journal*, *15*(6), 415–424.

Garrison, G., Kim, S., & Wakefield, R. (2012). Success factors for deploying cloud computing. *Communications of the ACM*, *55*(9), 62–68.

Garrity, J. T. (1963). Top management and computer profits. *Harvard Business Review*, *41*(4), 6–12.

Gartner. (2013). *Gartner Identifies the Top 10 Strategic Technology Trends for 2013*. Retrieved on the 21st of June 2015 from http://www.gartner.com/newsroom/id/2209615.

Gartner. (2015, August 26). *Forecast Analysis: Public Cloud Services, Worldwide, 2Q15 Update*. Retrieved on the 23rd of May, 2015 from https://www.gartner.com/doc/3119124/forecast-analysis-public-cloud-services.

Gartner. (2016, June 22). *Gartner Says By 2020, a Corporate "No-Cloud" Policy Will Be as Rare as a "No-Internet" Policy Is Today*. Retrieved on the 27th of December, 2016 from http://www.gartner.com/newsroom/id/3354117.

Gerber, M., & Von Solms, R. (2005). Management of risk in the information age. *Computers & Security*, *24*(1), 16–30.

Gewald, H., & Helbig, K. (2006). A governance model for managing outsourcing partnerships: A view from practice. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, Hawaii.

Ghauri, P. N., & Grønhaug, K. (2005). *Research methods in business studies: A practical guide*. London: Prentice Hall Financial Times.

Gibbs, G. R. (2002). *Qualitative data analysis: Explorations with NVivo*. Buckingham: Open University.

Glaser, B. G., & Strauss, A. L. (2009). *The discovery of grounded theory: strategies for qualitative research*. New Brunswick: Aldine.

Gold, R. S. (2002). Enabling the strategy-focused IT organization. *Information Systems Control Journal*, *4*, 21–24.

Gordijn, J., & van Eck, P. (2005). Value-Based Business-IT Alignment in Networked Constellations of Enterprises. In K. Cox, E. Dubois, Y. Pigneur, S. J. Bleistein, J. Verner, A. M. Davis, & R. J. Wieringa (Eds.), *1st International Workshop on Requirements Engineering for Business Need and IT Alignment (REBNITA 2005)* (pp. 38–43). New South Wales: University of New South Wales Press.

Gottschalk, P. (1999). Implementation Predictors of Strategic Information Systems Plan. *Information & Management*, *36*(2), 77–91.

Goundar, S. (2010). Cloud computing: Opportunities and issues for developing countries. *DiploFoundation: Internet Governance Research Paper*. Retrieved from http://www.academia.edu/download/13367072/igcbp2010_2011_goundar.pdf

Greener, S. 2008. *Business Research Methods*. Denmark: Bookboon, Ventus Publishing ApS. Retrieved on the 26th of March, 2016 from http://www.academybritish.co.uk/Library-eng/introduction-to-research-methods.pdf.

Gregor, S., Martin, M., Fernandez, W., Stern, S., & Vitale, M. (2006). The transformational dimension in the realization of business value from information technology. *The Journal of Strategic Information Systems*, *15*(3), 249–270.

Gu, B., Xue, L., & Ray, G. (2008). IT governance and IT investment performance: an empirical analysis. *Working Paper*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1145102

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. *Handbook of Qualitative Research*, *2*(163–194), 105–117.

Györy, A. A. B., Cleven, A., Uebernickel, F., & Brenner, W. (2012). Exploring the shadows: IT governance approaches to user-driven innovation. *Proceedings of the 22nd European Conference on Information Systems (ECIS)*, https://www.alexandria.unisg.ch/214625/1/ATTKL246.pdf

Haes, S. D., & Grembergen, W. V. (2008). Analysing the Relationship between IT Governance and Business/IT Alignment Maturity. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HCISS'08).*

Hardy, G. (2003). Coordinating IT Governance–A New Role for IT Strategy Committees. *Information Systems Control Journal*, *4*, 21–24.

He, Y. (2011). *The lifecycle process model for cloud governance (Master's Thesis)*. University of Twente. Belgium. Retrieved from http://essay.utwente.nl/61131/

Heart, T. (2010). Who is Out There? Exploring the Effects of Trust and Perceived Risk on SaaS Adoption Intentions. *The Data Base for Advances in Information Systems*, *41*(3), 49–68.

Henderson, J. C., & Venkatraman, H. (1993). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, *32*(1), 472–484.

Henderson, J. C., & Venkatraman, N. (1991). Understanding strategic alignment. *Business Quarterly*, *56*(3), 72–78.

Henderson, J. C., Thomas, J. B., & Venkatraman, N. (1992). *Making sense of it – strategic alignment and organizational context.* Cambridge, MA: Alfred P. Sloan School of Management, Massachusetts Institute of Technology.

Henderson, J., Venkatraman, N., & Oldach, S. (1993). Continuous Strategic Alignment, Exploiting Information Technology Capabilities for Competitive Success. *European Management Journal*, *11*(2), 139–149.

Herbsleb, J., Zubrow, D., Goldenson, D., Hayes, W., & Paulk, M. (1997). Software quality and the capability maturity model. *Communications of the ACM*, *40*(6), 30–40.

Héroux, S., & Fortin, A. (2012). The internal audit function in information technology governance: A holistic perspective. *Journal of Information Systems*, *27*(1), 189–217.

Hinz, D. J., & Malinowski, J. (2006). Assessing the Risks of IT Infrastructure—A Personal Network Perspective. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, Hawaii.

Hirschheim, R. (1985). Information systems epistemology: An historical perspective. In E. Mumford, R. Hirschheim, G. Fitzgerald, & T. Wood Harper (Eds.), *Research Methods in Information Systems*, Amsterdam: North-Holland Publishing Co.

Holden, M. T., & Lynch, P. (2004). Choosing the appropriate methodology: Understanding research philosophy. *The marketing review*, *4*(4), 397–409.

Holt, A., Weiss, K., Huberty, K., Gelblum, E., Flannery, S., Devgan, S., ... & Meunier, F. (2011). *Cloud Computing Takes Off: Market set to boom as migration accelerates*. Morgan Stanley Blue Paper. Retrieved on the 19th of April, 2015 from https://www.morganstanley.com/views/perspectives/cloud_computing.pdf.

Hon, W., Millard, C., & Walden, I. (2012). Negotiating cloud contracts: Looking at clouds from both sides now. *Stanford Technology Law Review*, *16*, 79.

Horlacher, A., & Hess, T. (2016, January). What does a Chief Digital Officer do? Managerial tasks and roles of a new C-level position in the context of digital transformation. *Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS)*, Hawaii.

Hough, A. (2011, September 21). 'Disastrous' £11.4bn NHS IT programme tobe abandoned. *Telegraph.co.uk.* Retrieved on the 28th of May, 2016, from http://www.telegraph.co.uk/news/health/news/8780566/Disastrous-11.4bn-NHS-IT-programme-to-be-abandoned.html

Houghton, L., & Kerr, D. (2006). A study into the creation of feral information systems as a response to an ERP implementation within the supply chain of a large government-owned corporation. *International Journal of Internet and Enterprise Management*, *4*(2), 135–147.

Hsu, W.-H. L. (2012). Conceptual framework of cloud computing governance model-an education perspective. *IEEE Technology and Engineering Education (ITEE)*, *7*(2), 12–16.

Humphrey, W. (2005). Why Big Software Project Fail: The 12 Key Questions. *Journal of Defined Software Engineering*, *18*(3), 25–29.

Huuskonen, S., & Vakkari, P. (2013). "I Did It My Way": Social workers as secondary designers of a client information system. *Information Processing & Management*, *49*(1), 380–391.

Ibbs, C. W., & Kwak, Y. H. (2000). Assessing project management maturity. *Project Management Journal*, *31*(1), 32–43.

Info Law Group (2010, May 27). *What's in Google's SaaS Contract with the City of Los Angeles? Part One*. Retrieved on the 10th of March, 2016 from http://www.infolawgroup.com/2010/05/articles/cloud-computing-1/whats-in-googles-saas-contract-with-the-city-of-los-angeles-part-one/.

Innovation Value Institute. (2012). *IT-Capability Maturity Framework.* Retrieved on the 19th of December 2016 from: https://content.ivi.ie/sites/default//files/media/ITCMF%20Overview%204pager%20Web_1.pdf.

ISACA. (2009). *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives.* Retrieved on the 12th of March, 2015 from: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/cloud-computing-business-benefits-with-security-governance-and-assurance-perspective.aspx.

ITA – International Trade Administration. (2016). *2016 Top Markets Report Cloud Computing: A Market Assessment Tool for U.S Exporters*. Retrieved on the 21st of August, 2016 from: http://trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf.

ITGI – IT Governance Institute. (2000). *CobiT: Governance, Control and Audit for Information and Related Technology*. Retrieved on the 21st of August, 2015 from http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx.

ITGI – IT Governance Institute. (2001). *Board briefing on IT Governance (2nd edition)*. Retrieved on the 21st of August, 2015 from http://www.isaca.org/Content/ContentGroups/ITGI3/Resources1/Board-Briefing_on_IT_Governance/26904_Board_Briefing_final.pdf.

ITGI – IT Governance Institute. (2003). *Board Briefing on IT Governance (2nd Edition)*. Retrieved on the 11th of December, 2014 from https://www.oecd.org/site/ictworkshops/year/2006/37599342.pdf.

ITGI – IT Governance Institute. (2005). *COBIT 4.0*. Retrieved on the 29th of July, 2015 from http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=27263.

ITL Education Solutions Limited. (2005). *Introduction to Information Technology*. India: Pearson Education.

ITU – International Telecommunication Union. (2012). *Focus Group on Cloud Computing Technical Report*. Retrieved on the 30th of June, 2015 from https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-CLOUD-2012-P1-PDF-E.pdf.

Jaeger, P., Lin, J., & Grimes, J. (2008). Cloud Computing and Information Policy: Computing in a Policy Cloud?. *Journal of Information Technology & Politics, 5*(3), 269–283.

Janssen, M., & Joha, A. (2011). Challenges for adopting cloud-based software as a service (saas) in the public sector. *Proceedings of the 19th European Conference on Information Systems (ECIS)*, Hilsinki, Finland.

Jarvenpaa, S. L., & Ives, B. (1991). Executive involvement and participation in the management of information technology. *MIS Quarterly*, *15*(2), 205–227.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, *3*(4), 305–360.

Jensen, M. C., & Meckling, W. H. (1995). Specific and general knowledge and organizational structure. *Journal of Applied Corporate Finance*, *8*(2), 4–18.

Jewer, J., & McKay, K. (2012). Antecedents and consequences of Board IT governance: Institutional and strategic choice perspectives. *Journal of the Association for Information Systems*, *13*(7), 581–617.

Joha, A., & Janssen, M. (2012). Transformation to Cloud Services Sourcing: Required IT Governance Capabilities. *ICST Transactions on E-Business*, *12*(7–9), https://repository.tudelft.nl/islandora/object/uuid:02362186-680b-4ca0-8d3a-72b91bab3a97/datastream/OBJ.

Johnstone, D., Huff, S., & Hope, B. (2006, January). IT projects: Conflict, governance, and systems thinking. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, Hawaii.

Jones, D., Behrens, S., Jamieson, K., & Tansley, E. (2004). The rise and fall of a shadow system: Lessons for enterprise system implementation. *Proceedings of the 15th Australasian Conference on Information Systems (ACIS)*, Hobart, Australia.

Kalyvas, J., Overly, M., & Karlyn, M. (2013). Cloud computing: A practical framework for managing cloud computing risk-part II. *Intellectual Property & Technology Law Journal*, *25*(4), 19–27.

Kaner, M., & Karni, R. (2004). A capability maturity model for knowledge-based decision making. *Information Knowledge Systems Management*, *4*(4), 225–252.

Kang, S., Myung, J., Yeon, J., Ha, S. W., Cho, T., Chung, J. M., & Lee, S. G. (2010). A general maturity model and reference architecture for saas service. In Z. Bao, G. Trajcevski, L. Chang, W. Hua, (Eds.), *Database Systems for Advanced Applications*, (pp. 337-346). Switzerland: Springer International Publishing.

Karimi, J., Bhattacherjee, A., Gupta, Y. P., & Somers, T. M. (2000). The Effect of MIS Steering Committees on Information Technology Management Sophistication. *Journal of Management Information Systems, 17*(2), 207–230.

Kearns, G. S., & Lederer, A. L. (2003). A resource-based view of strategic IT alignment: how knowledge sharing creates competitive advantage. *Decision Sciences, 34*(1), 1–29.

Keen, P. (1993). Information technology and the management difference: a fusion map. *IBM Systems Journal*, *32*(1), 17–39.

Kerr, D. V., Houghton, L., & Burgess, K. (2007). Power relationships that lead to the development of feral systems. *Australasian Journal of Information Systems*, *14*(2), 141–152.

Khalil, C., & Fernandez, V. (2013). Agile management practices in a lightweight organization: a case study analysis. *The Journal of Modern Project Management*, *1*(1).

Killalea, T. (2008). Building scalable Web services. *Queue*, *6*(6), 10–13.

Kim, W. (2009). Cloud computing: Today and tomorrow. *Journal of Object Technology*, *8*(1), 65–72.

Kirsch, L. J., & Beath, C. M. (1996). The enactments and consequences of token, shared, and compliant participation in information systems development. *Accounting, Management and Information Technologies*, *6*(4), 221–254.

Klein, H. K., & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly*, *23*(1), 67–93.

Kleinrock, L. (2005). A vision for the Internet. *ST Journal of Research*, *2*(1), 4–5.

Klesel, M., Mokosch, G., & Niehaves, B. (2015). Putting flesh on the Duality of Structure: the case of IT Consumerization. *Proceedings of the 21st Americas Conference on Information Systems (AMCIS)*, Puerto Rico.

Kopper, A., & Westner, M. (2016). Deriving a Framework for Causes, Consequences, and Governance of Shadow IT from Literature. *Proceedings of the Multikonferenz Wirtschaftsinformatik (MKWI)*.

Korac-Kakabadse, N., & Kakabadse, A. (2001). IS/IT governance: Need for an integrated model. *Corporate Governance: The international journal of business in society*, *1*(4), 9–11.

Kretzer, M., & Maedche, A. (2014). Generativity of Business Intelligence Platforms: A Research Agenda Guided by Lessons from Shadow IT. *Proceedings of the Multikonferenz Wirtschaftsinformatik.*

Kuhn, T. S. (1974). Second thoughts on paradigms. *The Structure of Scientific Theories*, *2*, 459–482.

Kundra, V. (2011). *Federal cloud computing strategy*. Washington D.C: The White House Retrieved on the 1st of April, 2015 from https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf

Kwon, D., & Watts, S. (2006). IT valuation in turbulent times. *The Journal of Strategic Information Systems*, *15*(4), 327–354.

Lacity, M. C., & Willcocks, L. (2000). *Global information technology outsourcing: In search of business advantage*. Hoboken, NJ: John Wiley & Sons, Inc.

Lahrmann G., Marx F., Winter R., & Wortmann F. (2011). Business Intelligence Maturity: Development and Evaluation of a Theoretical Model. *Proceedings of the 44th Annual Hawaii International Conference on System Sciences (HICSS'11)*, Hawaii.

Lapon, J. L. (1999). *La direction informatique et le pilotage de l'entreprise*. France: Hermès Science.

Lasica, J. D. (2009). *Identity in the age of cloud computing*. Santa Barbara, CA: The Aspen Institute.

Lawrence, P. R., & Lorsch, J. W. (Eds.). (1970). *Organizational structure and design*. Pittsburg, PA: RD Irwin.

Lazic, M., Groth, M., Schillinger, C., & Heinzl, A. (2011, August). The Impact of IT Governance on Business Performance. *Proceedings of the Americas Conference on Information Systems (AMCIS)*, Detroit.

Lee, J., & Lee, C. (2008). IT Governance-Based IT Strategy and Management: Literature Review and Future. In A. Cater-Steel (Ed.), *Information Technology Governance and Service Management: Frameworks and Adaptations*. Hershey, New York: IGI Global.

Lee, N. G. (1991). *Using computers in qualitative research*. Thousand Oaks, CA: SAGE Publications.

Leedy, P., & Ormrod, J. (2001). *Practical research: Planning and design* (7th Ed.). Thousand Oaks: SAGE Publications.

Leimeister, S., Böhm, M., Riedl, C., & Krcmar, H. (2010). The Business Perspective of Cloud Computing: Actors, Roles and Value Networks. *Proceedings of the 18th European Conference on Information Systems (ECIS)*, Pretoria, South Africa.

Levine, R. (2004). Risk Managemnt Systems: Understanding the Need. *Information Systems Management*, *21*(2), 31–37.

Lockamy III, A., & McCormack, K. (2004). The development of a supply chain management process maturity model using the concepts of business process orientation. *Supply Chain Management: An International Journal*, *9*(4), 272–278.

Luecke, R. (2003). *Managing Change and Transition*. Boston: Harvard Business School Press.

Luftman, J. & T. Brier (1999). Achieving and sustaining business-IT alignment. *California Management Review*, *42*(1), 109–122.

Luftman, J. (2000). Assessing Business-IT Alignment Maturity. *Communications of AIS*, *4*(14), 99–151.

Luftman, J. and Zadeh, H. (2011). Key Information Technology and Management Issues 2010–11: An international study. *Journal of Information Technology, 26*(3), 193–204.

Luftman, J. N. (2003). *Competing in the information age: Align in the sand*. United Kingdom: Oxford University Press.

Luftman, J. N., Lewis, P. R., & Oldach, S. H. (1993). Transforming the enterprise: The alignment of business and information technology strategies. *IBM Systems Journal*, *32*(1), 198–221.

Luftman, J., Zadeh, H. S., Derksen, B., Santana, M., Rigoni, E. H., & Huang, Z. (2012). Key information technology and management issues 2011–2012: an international study. *Journal of Information Technology*, *27*(3), 198–212.

Lyytinen, K., & Newman, M. (2015). A tale of two coalitions–marginalising the users while successfully implementing an enterprise resource planning system. *Information Systems Journal*, *25*(2), 71–101.

Maes, R., Rijsenbrij, D., Truijens, O., & Goedvolk, H. (2000). *Redefining business: IT alignment through a unified framework (PrimaVera working paper; No. 2000-19).* Amsterdam: Universiteit van Amsterdam, Department of Information Management.

Malterud, K. (2001). Qualitative research: standards, challenges, and guidelines. *The lancet*, *358*(9280), 483–488.

Markus, M. (2004). Technochange management: Using IT to drive organizational change. *Journal of Information Technology*, *19*(1), 3–19.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing — The business perspective. *Decision Support Systems*, *51*(1), 176–189.

Marwaha, S., & Willmott, P. (2006). Managing for scale, speed, and innovation. *McKinsey Quarterly*, *4*, 87.

Mason, M. (2010, August). Sample size and saturation in PhD studies using qualitative interviews. *Forum qualitative Sozialforschung/Forum: qualitative social research*, *11*(3), 1–19.

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud security and privacy: an enterprise perspective on risks and compliance*. Sebastopol, CA: O'Reilly Media, Inc.

Maykut, P., & Morehouse, R. (1994). *Beginning qualitative research: A philosophic and practical guide*. London, UK: The Falmer Press.

McCabe, D. L., Trevino, L. K., & Butterfield, K. D. (1996). The Influence of Collegiate and Corporate Codes of Conduct on Ethics-related behavior in the Workplace. *Business Ethics Quarterly*, *6*(4), 461–476.

Mell, P., & Grance, T. (2009). The NIST definition of cloud computing. *National Institute of Standards and Technology*, *53*(6), 50–51.

Menon, N. M., & Lee, B. (2000). Cost control and production performance enhancement by IT investment and regulation changes: evidence from the healthcare industry. *Decision Support Systems*, *30*(2), 153–169.

Mettler, T., & Rohner, P. (2009, May). Situational maturity models as instrumental artifacts for organizational design. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*.

Meyer, M., Zarekow, R., & Kolbe, L. M. (2003). IT-Governance. *Wirtschaftsinformatik*, *45*(4), 445–448.

Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: A sourcebook. *Beverly Hills: SAGE Publications*.

Mingers, J. (2003). The paucity of multimethod research: a review of the information systems literature. *Information Systems Journal*, *13*(3), 233–249.

Moir, L. (2001). What do we mean by corporate social responsibility?. *Corporate Governance: The international journal of business in society*, *1*(2), 16–22.

Moran, J., & Brightman, B. (2001). Leading organizational change. *Career Development International*, *6*(2), 111–118.

Morgan, L. & Conboy, K. (2003). Key factor impacting cloud computing adoption. *Computing*, *46*(10), 97–99.

Musson, D. (2008). IT Governance: a critical review of the literature. In A. Cater-Steel (Ed.), *Information Technology Governance and Service Management: Frameworks and Adaptations*. Hershey, New York: IGI Global.

Myers, M. (1997). Qualitative research in information systems. *Management Information Systems Quarterly*, *21*(2), 241–242.

Myers, M., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization*, *17*(1), 2–26.

Narbaitz, R., & Teitelman, G. (1965). A histochemical study of sex inversion produced by estradiol in chick embryos. *Development*, *13*(1), 45–50.

Newton, N. (2010). The use of semi-structured interviews in qualitative research: strengths and weaknesses. *Exploring qualitative methods*, *1*(1), 1–11.

Nicholson, B., & Sahay, S. (2004). Embedded knowledge and offshore software development. *Information and organization*, *14*(4), 329–365.

Niessink, F. & Clerc, V. & Tijdink, T. & van Vliet, H. (2005). *The IT Service Capability Maturity Model*. Educators, Bilthoven, and Vrije University, The Netherlands.

Nolan, R. (1982). Managing Information Systems by Committee. *Harvard Business Review*, *66*, 72–79.

Noor, T. H., Sheng, Q. Z., Zeadally, S., & Yu, J. (2013). Trust management of services in cloud environments: Obstacles and solutions. *ACM Computing Surveys*, *46*(1), 12–47.

OAG - Office of Auditors General of Canada. (2006). Strengthening Aid Effectiveness—Canadian International Development Agency. Retrieved on the 28th of August, 2016 from http://www.oag-bvg.gc.ca/internet/English/parl_oag_200911_08_e_33209.html.

ODCA – Open Data Center Alliance. (2013). Open Data Center Alliance$^{SM}$ usage model: Cloud maturity model Rev. 2.5. Retrieved on the 16$^{th}$ of October, 2016 from https://opendatacenteralliance.org/docs/cloud_maturity_model_rev_2.5/

Olivé, A. (2007). *Conceptual modeling of information systems*. Berlin, Germany: Springer Science & Business Media.

Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *The Electronic Journal Information Systems Evaluation*, *14*(1), 110–121.

Olson, M., & Chervany, N. (1980). The Relationship Between Organizational Characteristics and the Structure of the Information Services Function. *MIS Quarterly*, *2*(4), 57–69.

Olympics ticket sales suspended (2007, October 31). *BBC News*. Retrieved on the 29$^{th}$ of April, 2016 from http://news.bbc.co.uk/1/hi/world/asia-pacific/7070446.stm.

Onwubiko, C. (2010). Security Issues to Cloud Computing. In N. Antonopoulos & L. Gillam (Eds.), *Cloud Computing* (pp. 271–288). London: Springer London.

Opdenakker, R. (2006, August). Advantages and disadvantages of four interview techniques in qualitative research. *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, 7(4). Retrieved on the 20th of April, 2016 from http://www.qualitative-research.net/index.php/fqs/article/viewArticle/175/391&sa=U&ei=FdsJTdDCGYOnrAer0YjVDg&ved=0CP4BEBYwXg&usg=AFQjCNEsC2J0wILvNuH7LEhQaA2znBkKvw.

Open Data Center Alliance (ODCA). (2016). Open Data Center Alliance[SM] usage model: Cloud maturity model Rev. 3.0. Retrieved on the 12th of October, 2016 from https://opendatacenteralliance.org/article/cloud-maturity-model-rev-3-0/.

Oredo, J. O., & Njihia, J. (2014). Challenges of cloud computing in business: Towards new organizational competencies. *International Journal of Business and Social Science*, *5*(3), 150–160.

Orlikowski, W. (1993). CASE tools as organizational change: Investigating incremental and radical changes in systems development. *MIS quarterly*, *17*(3), 309–340.

Orlikowski, W. J. (1992). The Duality of Technology: Rethinking the concept of technology in organisations. *Organization Science*, *3*(2), 398–427.

Orlikowski, W., & Baroudi, J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information systems research*, *2*(1), 1–28.

Pang, M. S. (2014). IT governance and business value in the public sector organizations—The role of elected representatives in IT governance and its impact on IT value in US state governments. *Decision Support Systems*, *59*, 274–285.

Papp, R. (1999). Business-IT alignment: productivity paradox payoff?. *Industrial Management & Data Systems*, *99*(8), 367-373.

Pareek, D. (2006). *Business Intelligence for telecommunications*. Boca Raton, FL: CRC Press.

Parent, M., & Reich, B. (2009). Governing information technology risk. *California Management Review*, *51*(3), 134–152.

Parent, M., & Reich, B. H. (2009). Governing information technology risk. *California Management Review*, *51*(3), 134–152.

Patton, M. Q. (2002). *Qualitative Research & Evaluation Methods*. Thousand Oaks, CA: SAGE Publications.

Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability maturity model, version 1.1. *IEEE software*, *10*(4), 18–27.

Peak, D., & Guynes, C. S. (2003). Improving information quality through IT alignment planning: A case study. *Information Systems Management*, *20*(4), 22–29.

Peppard, J., Edwards, C. & Lambert, R. (2011). Clarifying the Ambiguous Role of the CIO. *MIS Quarterly Executive*, *10*(4), 31–44.

Peterson, K. D., & Deal, T. E. (1998). How leaders influence the culture of schools. *Educational Leadership*, *56*(1), 28–31.

Peterson, R. (2004). Crafting information technology governance. *Information Systems Management*, *21*(4), 7–22.

Peterson, R. R., O'Callaghan, R., & Ribbers, P. (2000, December). Information technology governance by design: Investigating hybrid configurations and integration mechanisms. *Proceedings of the 21st International Conference on Information Systems*, Brisbane, Austria.

Pironti, J. P. (2006). Information security governance: Motivations, benefits and outcomes. *Information Systems Control Journal*, *4*, 45–48.

Poels, R. P. (2006). *Beïnvloeden en meten van business-IT alignment* (*Doctoral dissertation*). Vrije Universiteit Amsterdam. The Netherlands.

Porter, M. E. (1982). *Choix stratégiques et concurrence*. Paris, France: Economica.

Powell, A., & Yager, S. E. (2004). Exploring reputation differences in information systems groups. *Journal of Information Technology Case and Application Research*, *6*(2), 5–26.

Prasad, A., Green, P., & Heales, J. (2014). On governance structures for the cloud computing services and assessing their effectiveness. *International Journal of Accounting Information Systems*, *15*(4), 335–356.

Premkumar, G., & King, W. (1994). The Evaluation of Strategic Information System Planning. *Information & Management*, *26*(6), 327–340.

Quintero, D., Ceron, R., Dhandapani, M., Garcia da Silva, R., Ghosal, A., Hu, V., Chen Li, H., Marthi, K., Feng Shi, S., Velica, S. (2013). *IBM Technical Computing Clouds*. Retrieved on the 5th of June, 2015 from http://www.redbooks.ibm.com/redbooks/pdfs/sg248144.pdf.

Ragowsky, A., Licker, P., & Gefen, D. (2014, August). Organizational information technology maturity: Antecedent factors and consequent outcomes. *Proceedings of the 16th International Conference on Electronic Commerce*, Valencia, Spain.

Rajendran, S. (2013). *Organizational challenges in cloud adoption and enablers of cloud transition program (Doctoral Dissertation)*. Massachusetts Institute of Technology. Boston.

Rau, K. (2004). Effective governance of IT: Design objectives, roles, and relationships. *Information Systems Management*, *21*(4), 35–42.

Reeves, T. C., & Hedberg, J. G. (2003). *Interactive learning systems evaluation*. Englewood Cliffs, NJ: Educational Technology.

Reich, B. H., & Benbasat, I. (1996). Measuring the linkage between business and information technology objectives. *MIS Quarterly*, *20*(1), 55–81.

Reich, B., & Benbasat, I. (2000). Alignment between Business and IT Objectives. *MIS Quarterly, 24*(1), 81–113.

Reix, R., Fallery, B., Kalika, M., & Rowe, F. (2016). *Systèmes d'information et management*. Paris, France: Vuibert.

Renault touché par la cyberattaque international (2017, May 13). *Le Figaro*. Retrieved on the 27th of May, 2017 from http://www.lefigaro.fr/conjoncture/2017/05/13/20002-20170513ARTFIG00068-renault-touche-par-la-cyberattaque-internationale.php.

Ribbers, P. M., Peterson, R. R., & Parker, M. M. (2002). Designing information technology governance processes: diagnosing contemporary practices and competing theories. *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02).*

Ribbers, P. M., Peterson, R. R., & Parker, M. M. (2002, January). Designing information technology governance processes: diagnosing contemporary practices and competing theories. *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02),* Hawaii.

Ried, S., Kisker, H., Matzke, P., Bartels, A., & Lisserman, M. (2011). Sizing the Cloud, Understanding And Quantifying The Future Of Cloud Computing. *Forrester Research, Inc.*, *21*, 13.

Rockart, J. (1988). The Line Takes the Leadership. *MIT Sloan Management Review, 29*(4), 57–64.

Rosemann, M., & Debruin, T. (2005). Business process management maturity-a model for progression. *Proceedings of the 13th European Conference on Information Systems (ECIS),* Regensburg, Germany.

Ross, J. W. (2003). Creating a Strategic IT Architecture Competency: Learning in Stages. *MIT Sloan School for Management*. Retrieved on the 7th of November, 2014 from https://s3.amazonaws.com/academia.edu.documents/6369844/4314-03.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1504104003&Signature=S%2FZXElzJROGk5PNAZHcvCqgq1HA%3D&response-content-disposition=inline%3B%20filename%3DCreating_a_strategic_IT_architecture_com.pdf.

Ross, J. W., & Weill, P. (2002). Six IT decisions your IT people shouldn't make. *Harvard Business Review*, *80*(11), 84–95.

Ross, J. W., Beath, C. M., & Goodhue, D. L. (1996). Develop long-term competitiveness through IT assets. *Sloan Management Review*, *38*(1), 31–57.

Ross, J. W., Weill, P., & Robertson, D. (2006). *Enterprise architecture as strategy: Creating a foundation for business execution*. Brighton, MA: Harvard Business Press.

Ruohonen, M. (1991). Stakeholders of strategic information systems planning: theoretical concepts and empirical examples. *The Journal of Strategic Information Systems*, *1*(1), 15–28.

Sambamurthy, V. & Zmud, R. (2000). The Organizing Logic of IT Activities in the Digital Era: A Prognosis and a Call for Research. *Information Systems Research*, *11*(2), 105–114.

Sambamurthy, V., & Zmud, R. W. (1999). Arrangements for Information Technology Governance: A Theory of Multiple Contingencies. *MIS Quarterly*, *23*(2), 261–290.

Schalow, P. R., Winkler, T. J., Repschlaeger, J., & Zarnekow, R. (2013). The Blurring Boundaries Of Work-Related And Personal Media Use: A Grounded Theory Study On The Employee's Perspective. *Proceedings of the 21st European Conference on Information Systems (ECIS).*

Schmidt, P. and Grabski, S. (2015), Proposing a Cloud Computing Capability Maturity Model. Symposium 2015, Retrieved on the 18th of October, 2016 from http://jebcl.com/symposium/wp-content/uploads/2015/09/ID6_Grabski_Schmidt_Cloud-Capability-Maturity-Model.pdf.

Schmidt, R., Zimmermann, A., Möhring, M., Nurcan, S., Keller, B., & Bär, F. (2015, September). Digitization–perspectives for conceptualization. *Proceedings of the European Conference on Service-Oriented and Cloud Computing*, Taormina, Italy.

Schmitt, J., & Kozar, K. (1978). Management's Role in Information System Development Failures: A Case Study. *MIS Quarterly*, *2*(2), 7-16.

Schneider, S., & Sunyaev, A. (2016). Determinant factors of cloud-sourcing decisions: reflecting on the IT outsourcing literature in the era of cloud computing. *Journal of Information Technology*, *31*(1), 1–31.

Schuman, S. P., & Rohrbaugh, J. (1991). Decision Conference for Systems Planning. *Information & Management*, *21*(3), 147–159.

Schwarz, A., & Hirschheim, R. (2003). An extended platform logic perspective of IT governance: managing perceptions and activities of IT. *The Journal of Strategic Information Systems*, *12*(2), 129–166.

Sharma, A. (2012). IT Governance: Driven by Challenges of Corporate Governance. *International Journal of Computing & Business Research*. http://www.researchmanuscripts.com/isociety2012/34.pdf

Silverman, D. (2000). Analyzing talk and text. In N. Denzin & Y. Lincoln (Eds.), *Handbook of qualitative research*, (pp. 821–834). Thousand Oaks, CA: SAGE Publications.

Silvius, A. G. (2007, January). Business & IT Alignment in theory and practice. *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, Hawaii.

Simonsson, M., & Johnson, P. (2006). Defining IT governance-a consolidation of literature. *Proceedings of the 20th Conference on Advanced Information Systems Engineering*, Montpellier, France.

Simonsson, M., Johnson, P., & Ekstedt, M. (2010). The effect of IT governance maturity on IT governance performance. *Information systems management*, *27*(1), 10–24.

Simpson, J., & Weiner, E. S. (1989). *Oxford English dictionary online*. Oxford: Clarendon Press.

Singh, H. (2015). Emergence and Consequences of Drift in Organizational Information Systems. *Proceedings of the 19th Pacific Asia Conference on Information Systems (PACIS)*, Singapore, Singapore.

Sircar, S., Turnbow, J. L., & Bordoloi, B. (2000). A framework for assessing the relationship between information technology investments and firm performance. *Journal of Management Information Systems*, *16*(4), 69–97.

Skinner, D., Tagg, C., & Holloway, J. (2000). Managers and research: the pros and cons of qualitative approaches. *Management Learning*, *31*(2), 163–179.

Sky High. (2016). *Cloud Adoption and Risk Report*. Retrieved from: https://www.skyhighnetworks.com/cloud-report/ on the 17th of May, 2015.

Smaczny, T. (2001). Is an alignment between business and information technology the appropriate paradigm to manage IT in today's organisations?. *Management Decision*, *39*(10), 797–802.

Software Engineering Institute. (2002). Capability Maturity Model® Integration (CMMISM), Version 1.1. *Staged Representation*.

Sohal, A. S., & Fitzpatrick, P. (2002). IT Governance and Management in Large Australian Organizations. *International Journal of Production Economics*, *75*(1–2), 97–112.

Spierings, A., Kerr, D., & Houghton, L. (2014). What Drives the End User to Build a Feral Information System?. In D. Kerr, K. Burgess, & L. Houghton (Eds.), *Feral Information Systems Development: Managerial Implications*. Hershey, PA: IGI Global.

Srinivasan, S. (2013). Is security realistic in cloud computing? *Journal of International Technology and Information Management*, *22*(4), 47–66.

Stake, R. E. (1995). *The art of case study research*. Thousand Oaks, CA: SAGE Publications.

Standards Australia. (2004). *Risk Management Standard*. Retrieved from: https://infostore.saiglobal.com/store/getpage.aspx?path=/publishing/shop/promotions/AS_NZS_ISO_31000:2009_Risk_Management_Principles_and_guidelines.htm&site=RM on the 4th of July, 2015.

Standing, C., Guilfoyle, G., Lin, C., & Love, P. (2006). The Attribution of Success and Failure in IT Projects. *Industrial Management and Data Systems*, *106*(8), 1148–1165

Standish Group (2010). *Chaos Summary for 2010*. Retrieved from. https://cours.etsmtl.ca/mti515/notes/cours01/chaos%20summary%202010.pdf on the 20th of June, 2017.

Standish Report (2015). *Chaos Summary for 2015*. Retrieved from: https://www.culture-agile.com/chaos-report-2015/ on the 20th of June 2017.

Stanoevska-Slabeva, K., & Wozniak, T. (2010). Cloud basics–an introduction to cloud computing. In K. Stanoevska-Slabeva, T. Wozniak, & S. Ristol (Eds.), *Grid and cloud computing* (pp. 47–61). Berlin, Germany: Springer Heidelberg.

Starre, D., & De Jong, B. (1998). *IT Governance and Management*. Nolan: Norton & Co.

Stewart, A. (2004). On risk: perception and direction. *Computers & Security*, *23*(5), 362–370.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research* (Vol. 15). Thousand Oaks, CA: SAGE Publications.

Strnadl, C. F. (2006). Aligning business and it: The process-driven architecture model. *Information Systems Management*, *23*(4), 67–77.

Su, N. (2011). Emergence of cloud computing: an institutional innovation perspective. *Proceedings of the 32nd International Conference on Information Systems (ICIS)*, Shanghai, China.

Sultan, N. A. (2011). Reaching for the "cloud": How SMEs can manage. *International Journal of Information Management*, *31*(3), 272–278.

Sun, L., Srivastava, R. P., & Mock, T. J. (2006). An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. *Journal of Management Information Systems*, *22*(4), 109–142.

Susarla, A., Barua, A., & Whinston, A. B. (2003). Understanding the service component of application service provision: empirical analysis of satisfaction with ASP services. *MIS Quarterly*, *27*(1), 91–123.

Svensson, H., & Host, M. (2005). Views from an organization on how agile development affects its collaboration with software development team. *International Conference on Product Focused Software Process Improvement*, Oulu, Finland.

Tallon, P. Kraemer, K. & Gurbaxani, V. (2000). Executives' perceptions of the business value of information technology: a process-oriented approach. *Journal of Management Information Systems*, *16*(4), 145–173.

Tallon, P. P. (2007). A process-oriented perspective on the alignment of information technology and business strategy. *Journal of Management Information Systems*, *24*(3), 227–268.

Tallon, P. P., & Kraemer, K. L. (2003). Investigating the relationship between strategic alignment and IT business value: the discovery of a paradox. In N. Shin

(Ed.), *Creating Business Value with Information Technology: Challenges and Solutions*, (pp. 1–22). Hershey, PA: IGI Global Publishing.

Tanks in the Clouds (2010, December 29). *The Economist.* Retrieved on the 28th of May, 2016 from http://www.economist.com/node/17797794.

Tavakolian, H. (1989). Linking the Information Technology Structure with Organizational Competitive Strategy: A Survey. *MIS Quarterly*, *13*(3), 309–317.

Taylor, A. (2000). IT projects: sink or swim. *ITNOW*, *42*(1), 24–26.

Teece, D. (2007). Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, *28*(13), 1319–1350.

Thatcher, M. E., & Pingry, D. E. (2007). Modeling the IT value paradox. *Communications of the ACM*, *50*(8), 41–45.

Thatte, S., Grainger, N., & McKay, J. (2012). Feral practices. *Proceedings of the 23rd Australasian Conference on Information Systems (ACIS)*, Australia.

The Defense Science Board. (2013). *Cyber Security and Reliability in a Digital Cloud*. Retrieved from the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (Washington D.C.).

Tiers–Gregoire, G., Mourmant, G., & Leclercq-Vandelannoitte, A. (2014). L’envol vers le cloud : un phénomène de maturations multiples. *Systèmes d’Information et Management*, *18*(4).

Tiwana, A. (2009). Governance-Knowledge Fit in Systems Development Projects. *Information Systems Research*, *20*(2), 180–197.

Tran, S. (2012). Le pilotage des entreprises étendues: le rôle du SI dans le dispositif de gestion. *Finance Contrôle Stratégie*, *15*(1/2).

Tran, S., & Bertin, E. (2016). Changing organizational models of IT departments as a result of cloud computing: proposal for a typology. *Systèmes d'information & management*, *20*(4), 51–87.

Trevino, L., Weaver, G., Gibson, D., & Toffler, B. (1999). Managing Ethics and Legal Compliance: What Works and What Hurts. *California Management Review, 41*(2), 131–151.

Turban, E., Rainer, R. K., & Potter, R. E. (2001). *Introduction to information technology*. New York: John Wiley.

Urbach, N., Buchwald, A., & Ahlemann, F. (2013). Understanding IT Governance Success And Its Impact: Results From An Interview Study. *Proceedings of the 21st European Conference on Information Systems (ECIS*), Utrecht, The Netherlands.

Van der Aalst, W. M., & Stahl, C. (2011). *Modeling business processes: a petri net-oriented approach*. Cambridge: MIT Press.

Van Grembergen, W. (2002). IT Governance and Its Mechanisms. *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02)*, Hawaii.

Van Grembergen, W., & De Haes, S. (2009). *Enterprise governance of information technology: achieving strategic alignment and value*. Berlin, Germany: Springer Science & Business Media.

Van Grembergen, W., & Van Bruggen, R. (1997, October). Measuring and improving corporate information technology through the balanced scorecard technique. *Proceedings of the 4th European Conference on the Evaluation of Information technology* , Delft, The Netherlands.

Van Grembergen, W., De Haes, S., & Guldentops, E. (2004). Structures, processes and relational mechanisms for IT governance. *Strategies for Information Technology Governance, 2*(4), 1–36.

Van Grembergen, W., De Haes, S., & Van Brempt, H. (2007, January). Prioritising and linking business and IT goals in the financial sector. *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, Hawaii

Vaswani, R. (2003). *Determinants of Effective Information Technology (IT) Governance* (*Unpublished dissertation*). School of Business, University of Queensland. Australia.

Venters, W. & E. Whitley (2012). A critical review of cloud computing: researching desires and realities. *Journal of Information Technology*, *27*(3), 179–197.

VersionOne, Inc. (2016). *10th annual "state of agile development" survey* [Data File]. Retrieved on the 4th of March, 2017 from http://www.agile247.pl/wp-content/uploads/2016/04/VersionOne-10th-Annual-State-of-Agile-Report.pdf.

Vishwakarma, A. K. (2012). Cloud Computing: Future Generation Computing Systemsas the 5th Utility. *International Journal of Information and Electronics Engineering*, *2*(2), 193–196.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371-376.

Voorsluys, W., Broberg, J., & Buyya, R. (2011). Introduction to Cloud Computing. In R. Buyya, J. Broberg and A. Goscinsk (Eds.), *Cloud Computing: Principles and Paradigms* (pp. 1–44). Hoboken, NJ: John Wiley & Sons, Inc.

Vouk, M. (2008). Cloud Computing – Issues, research and implications. *Journal of Computing and Information Technology*, *16*(4), 235–246.

Wagner, H. T., Beimborn, D., Franke, J., & Weitzel, T. (2006, January). IT business alignment and IT usage in operational processes: a retail banking case. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, Hawaii.

Walsham, G. (1995). Interpretive case studies in IS research: nature and method. *European Journal of information systems*, *4*(2), 74–81.

Walterbusch, M., Fietz, A., & Teuteberg, F. (2014). Schatten-IT: Implikationen und Handlungsempfehlungen für Mobile Security. *HMD Praxis der Wirtschaftsinformatik*, *51*(1), 24–33.

Walters, R. (2013). Bringing IT out of the shadows. *Network Security*, 2013(4), 5–11.

Wang, P., & Ramiller, N. C. (2009). Community learning in information technology innovation. *MIS Quarterly*, 709–734.

Webb, P., Pollard, C. & Ridley, G. (2006). Attempting to Define IT Governance: Wisdom or Folly?. *Proceedings of the 39th Hawaii International Conference on System Sciences (HICSS'06)*, Hawaii.

Wei, J., Zhang, X., Ammons, G., Bala, V., & Ning, P. (2009). Managing security of virtual machine images in a cloud environment. *Proceedings of the 2009 ACM workshop on Cloud Computing Security*.

Weill, P. & Ross, J.W. (2004). *IT Governance - How Top Performers Manage It Decision Rights for Superior Results*. Boston: Harvard Business School Press.

Weill, P. & Woerner, S. (2013). The Future of the CIO in a Digital Economy. *MIS Quarterly Executive*, *12*(2), 65–75.

Weill, P. (2004). Don't just lead govern: How top performing firms govern IT. *MIS Quarterly Executive*, *3*(1), 1–17.

Weill, P., & Broadbent, M. (1998). *Leveraging the new infrastructure: how market leaders capitalize on information technology*. Boston: Harvard Business School Press.

Weill, P., & Woodham, R. (2002). Don't just lead, govern: Implementing effective IT governance. *MIT Sloan School of Management*.

Westerman, G., & Weill, P. (2004). What are the Key Capabilities of Effective CIOs?, Cambridge: Center for Information Systems Research, MIT. Retrieved on the 17th of March, 2015 from http://cisr.mit.edu/blog/documents/2004/10/22/2004_10_3c_keycapabilitieseffcio-pdf/.

Wiens, T., & Ullrich, C. A. (2016). *Scheduling with Team Production Effects*. Retrieved on the 29th of June from SSRN: https://ssrn.com/abstract=2781470.

Wilkin, C. L., & Chenhall, R. H. (2010). A review of IT governance: A taxonomy to inform accounting information systems. *Journal of Information Systems*, *24*(2), 107–146.

Winkler, T., & Brown, C. (2014). Horizontal Allocation of Decision Rights for On-Premise Applications and Software-as-a-Service. *Journal of Management Information Systems*, *30*(3), 13–48.

Winkler, T., Benlian, A., Piper, M., & Hirsch, H. (2014). Bayer HealthCare Delivers a Dose of Reality for Cloud Payoff Mantras in Multinationals. *MIS Quarterly Executives*, *13*(4), 193–208.

Xue, Y., Liang, H., Boulton, W. (2008). Information Technology Governance in Information Technology Investment Decision Processes: The Impact of Investment Characteristics, External Environment, and Internal Context. *MIS Quarterly*, *32*(1), 67–96.

Yanosky, R., & Caruso, J. B. (2008). Process and politics: IT governance in higher education. *ECAR Key Findings*. Retrieved on the 17th of May, 2015 from http://www-cdn.educause.edu/ir/library/pdf/EKF/EKF0805.pdf.

Yeboah-Boateng, E. O., & Essandoh, K. A. (2014). Factors influencing the adoption of cloud computing by small and medium enterprises in developing economies. *International Journal of Emerging Science and Engineering*, *2*(4), 13–20.

Yeo, K., & Ren, Y. (2009). Risk management capability maturity model for complex product systems (CoPS) projects. *Systems Engineering*, *12*(4), 275–294.

Yin, R. K. (2003). Case study research: Design and methods (3rd ed.). Thousand Oaks, CA: SAGE Publications.

Young, R. C., Jordan, E. (2002). IT Governance and Risk Management: an integrated multi-stakeholder framework. *Asia Pacific Decision Sciences Institute, Bangkok, Thailand*.

Zainuddin, E. (2012). Secretly saas-ing: stealth adoption of software-as-a-service from the embeddedness perspective. *Proceedings of the 33rd International Conference on Information Systems (ICIS)*, Orlando, USA.

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.

Zimmermann, S., & Rentrop, C. (2014). On the Emergence of Shadow IT: A Transaction Cost-Based Approach. *Proceedings of the 22nd European Conference on Information Systems (ECIS)*, Tel Aviv, Israel.

# Appendices

## I. Round I – Semi Structured Interview Guide

1. Can you please start with introducing your company?
2. As mentioned in the emails, your organization adopts cloud services?
3. Which deployment models are you adopting?
    a. Public? Private? Hybrid?
4. Which service models are you adopting?
    a. SaaS? PaaS? IaaS?
5. What is the strategy behind adopting cloud services in your organization
    a. Innovation? Reduction of costs? Competition? Agility? Other?
6. What are your expectations from adopting cloud services? What are the benefits behind it?
7. Do risks emerge from the adoption of cloud services?
    a. What types of risks? How do you mitigate them?
8. Which contingency factors in your organization impact the adoption of the cloud?
9. What are the different cloud decisions that the organization has addressed during regular meetings?
10. How do you perceive your organization's IT is mostly governed?
    a. Through a Centralization? Decentralization? Federal?
11. How is the role of the IT department affected by the digital wave?
12. Who takes cloud-related decisions? Is it through discussions and collaboration?
13. During the adoption of cloud services, did your organization witness
    a. Any additional decision-making structures related to the cloud?
    b. Any additional business processes related to the cloud?
    c. Any additional relational mechanisms related to the cloud?
    d. Could you please elaborate them?
14. How does the adoption of cloud services affect your organization? Can you elaborate by giving examples?
15. Do you witness "shadow IT" activities with the adoption of cloud services?
16. It was shown that the cloud brings standardization, how do your business departments differentiate themselves from others?

17. In the near future, what vision do you have regarding the cloud? Will it lead to more innovation (IoT, for example?)

# II. Round II – Questions of Structured Interview Guide

## 1. Strategy Domain

- **Q1**: Does a formal enterprise level strategy exist positioning the use of cloud based services?
- **Q2**: Is there a Cloud Adoption Framework?
- **Q3**: Do Key Performance Indicators exist for cloud based services?

## 2. Organization and Skills Domain

- **Q4**: Has the organizational structure been updated to enable Cloud based Service delivery?
- **Q5**: Is a formal Cloud Training planned?
- **Q6**: What is the role of Internal IT?

## 3. Governance Domain

- **Q7**: Does a formal Communication plan exist, positioning cloud and the impacts?
- **Q8**: Is Risk Management updated for Cloud?
- **Q9**: Is there a formal Compliance framework for Cloud?
- **Q10**: Do Cloud Contract templates exist?

## 4. Project, Portfolio and Services Domain

- **Q11**: Are Project Tools updated to support Cloud projects?
- **Q12**: Do Project Skills exist for cloud projects?

## 5. Architecture Domain

- **Q13**: Are Architecture Processes in existence for Cloud based services?

## 6. Operations Domain

- **Q14**: Are clear processes (e.g. ITIL) for service, risk and compliance management processes defined for cloud based services including Incident, Problem and Change Management, and integrated with the consumer ecosystems?

## 7. Infrastructure Domain

- **Q15**: For organizations adopting IaaS solutions; Is monitoring updated for IaaS Cloud based services?
- **Q16**: For organizations adopting PaaS solutions; Is a PaaS framework available for the business to leverage for effective cloud application development?
- **Q17**: For organizations adopting SaaS solutions; Does an enterprise policy exist for the use of SaaS services and the resulting data sets?

## 8. Information Domain

- **Q18**: Are Security Skills updated to include Cloud solutions?

# III. NVivo Word Frequency

| Words | Frequency | Words | Frequency | Words | Frequency |
|---|---|---|---|---|---|
| cloud | 1378 | directions | 52 | management | 29 |
| données | 312 | fournisseurs | 52 | qualité | 29 |
| métiers | 203 | compliqué | 51 | société | 29 |
| services | 189 | développement | 51 | techniques | 29 |
| entreprises | 180 | iaas | 51 | prestataire | 28 |
| clients | 179 | risque | 51 | usages | 28 |
| sécurité | 178 | structures | 50 | vision | 28 |
| besoin | 146 | technologies | 50 | cdo | 27 |
| système | 135 | application | 49 | confidentialité | 27 |
| data | 132 | fournisseur | 49 | impact | 27 |
| business | 128 | microsoft | 48 | directeur | 26 |
| saas | 120 | serveur | 48 | développer | 26 |
| numérique | 111 | internet | 47 | ibm | 26 |
| france | 108 | problèmes | 47 | l'entreprise | 26 |
| projet | 107 | stratégie | 47 | sociale | 26 |
| entreprise | 103 | décisions | 46 | sociétés | 25 |
| solution | 100 | l’informatique | 46 | capex | 24 |
| privé | 98 | ressources | 46 | communication | 24 |
| direction | 91 | contrat | 43 | d’entreprise | 24 |
| processus | 88 | sap | 43 | plateforme | 24 |
| amazon | 83 | coûts | 42 | politique | 24 |
| applications | 81 | infrastructure | 42 | publique | 24 |
| gouvernance | 80 | messagerie | 41 | utilisateurs | 24 |

| | | | | | |
|---|---|---|---|---|---|
| digital | 78 | organisations | 41 | équipe | 24 |
| d'information | 77 | départements | 40 | classique | 23 |
| informatique | 76 | informatiques | 40 | puissance | 23 |
| marché | 75 | paas | 40 | démarche | 22 |
| l'it | 73 | payer | 40 | l'infrastructure | 22 |
| serveurs | 73 | décision | 38 | prive | 22 |
| outils | 71 | questions | 38 | responsable | 22 |
| systèmes | 71 | réversibilité | 38 | commerce | 21 |
| public | 69 | stratégique | 38 | domaines | 21 |
| gestion | 67 | acteurs | 37 | expérience | 21 |
| risques | 66 | logiciels | 37 | legacy | 21 |
| changer | 65 | officer | 37 | numériques | 21 |
| google | 64 | contrats | 36 | outil | 21 |
| production | 63 | budget | 35 | pilotage | 21 |
| transformation | 63 | technologie | 35 | prestation | 21 |
| infrastructures | 59 | changement | 34 | règles | 21 |
| marketing | 59 | chief | 34 | donnees | 20 |
| compétences | 58 | capacité | 33 | maintenance | 20 |
| offre | 56 | l'impact | 33 | protection | 20 |
| technique | 55 | relations | 33 | salariés | 20 |
| besoins | 54 | réseaux | 33 | accès | 19 |
| comité | 53 | produit | 32 | agile | 19 |
| logiciel | 53 | stockage | 32 | attention | 19 |
| process | 53 | l'agilité | 30 | concurrence | 19 |
| salesforce | 53 | difficile | 29 | financière | 19 |

| | | | | | |
|---|---|---|---|---|---|
| valeur | 53 | domaine | 29 | l’intérêt | 19 |
| acheter | 52 | français | 29 | médias | 19 |

# French Summary

**RESUME :** L'avènement de l'internet a entraîné des changements majeurs dans les entreprises ces dernières décennies. De nouveaux modèles d'affaires et services ont émergé affectant les processus métiers et les modes de fonctionnement au sein des entreprises. L'adoption des solutions cloud n'a fait qu'accentuer ces transformations. Si ces solutions ont permis d'améliorer l'automatisation des processus, d'accroître l'agilité organisationnelle, de réduire le time-to-market, et d'assurer des services informatiques à la demande, elles ont également engendré de nouveaux risques pour les entreprises liés à la sécurité, la fiabilité des services, et même la nécessité de nouvelles compétences spécifiques. Comme pour la gouvernance des TIC, les entreprises doivent gouverner leurs solutions cloud afin d'en tirer le maximum davantage et de réduire les risques associés. Bien que de nombreux travaux se soient intéressés à la gouvernance des TIC, peu se sont penchés sur la manière dont les entreprises gouvernent leurs solutions cloud. A cet effet, nous avons décidé de mener une étude qualitative, basés sur la conduite d'entretiens, auprès de 35 grandes entreprises françaises ayant adopté des solutions cloud. Cette étude nous a permis d'explorer les modèles de gouvernance déployés dans les entreprises françaises et d'identifier les liens éventuels entre le modèle de gouvernance déployé et les niveaux d'intensité d'adoption des solutions cloud. Ce travail de thèse met en évidence les différents impacts liés à l'adoption du cloud et souligne l'émergence de plusieurs modèles de gouvernance au sein des entreprises interrogées. Cependant différents facteurs de contingence semblent influencer ces modèles de gouvernance.

# Sommaire

# Introduction

***C***=299 792 458 m/s. Cette valeur représente la vitesse de la propagation de la lumière dans le vide. Nous ne pouvons nier que ***C*** représente une vitesse hors de portée. Mais, nous pouvons sans doute dire que nous sommes témoins de l'évolution de l'ère digitale et de sa propagation à une vitesse proche de celle-ci. Au cours des dernières décennies, la société a témoigné d'une évolution imposante en termes de technologies. L'ordinateur, par exemple, est passé de la taille d'un appartement (de banlieue et non parisien) à un ordinateur portable pesant 300g. Ces dernières années ont aussi vu les technologies de l'information et de la communication (TIC), devenir indispensables à la plupart de nos activités quotidiennes.

Les TIC regroupent les moyens de traitement et de transmission de l'information et représentent dans une entreprise des outils incontournables pour son fonctionnement et son succès. En revanche, afin de bénéficier des avantages apportés par les TIC au sein de l'entreprise, il est nécessaire de les gouverner. D'une part, plusieurs travaux de recherche montrent le lien entre le manque de gouvernance et la faillite des entreprises (Frost, 1992 ; Daily et Dalton, 1994 ; Fich et Skelzak, 2008) et d'autre part, un plus grand nombre d'études exposent les effets positifs de la gouvernance des TIC pour les entreprises, comme une hausse de la performance, un avantage concurrentiel, ou un service clientèle amélioré (Sambamurthy et Zmud, 2000 ; Reich et Benbasat, 2000 ; Weill et Ross, 2004 ; Brown et Grant, 2005 ; Tallon et al., 2000). Ceci incite les entreprises à appliquer une gouvernance effective afin de bénéficier de toutes ces opportunités. Elles doivent donc se demander ce qui définit une gouvernance effective des TIC et comment adopter une telle gouvernance. Les travaux antérieurs avaient comme objectif de définir la gouvernance effective ainsi que les étapes à suivre afin de faciliter son adoption pour les entreprises. Selon Weill et Ross (2004), De Haes et Van Grembergen (2004), et Peterson (2004), elles doivent passer par trois étapes nécessaires : tout d'abord, les parties-prenantes de l'entreprise doivent inclure des décisions adressant divers aspects de l'entreprise. Ensuite, une fois les décisions sont discutées, elles doivent être allouées aux décideurs les plus appropriés. Enfin, l'entreprise doit mettre en place de nombreux mécanismes de gouvernance, tels que des structures liées à la prise de décisions, des processus *business*, et des mécanismes relationnels, afin de faciliter l'implémentation des décisions.

Comme mentionné, le monde digital se propage à très grande vitesse, donnant naissance à une myriade de nouvelles technologies telles que les solutions *cloud*. Le *cloud* est devenu un sujet largement abordé par les travaux de recherche dans le domaine des Systèmes d'Informations, qui ont étudié son émergence rapide au sein des entreprises. Malgré les nombreuses opportunités apportées par les solutions cloud, leur adoption est freinée par une longue liste de risques qu'elles génèrent. Par conséquent, afin de bénéficier de ses avantages tout en évitant ses risques, les entreprises sont conseillées de bien les gouverner. Néanmoins, rares sont les études proposant un modèle de gouvernance du *cloud* se penchant sur tous les aspects des solutions *cloud*. Toutefois, alors que les solutions *cloud* font partie des TIC d'une entreprise, peuvent-elles donc être simplement gouvernées en s'appuyant sur la gouvernance usuelle des TIC ?

Ceci nous pousse à nous poser la question suivante : *Le déploiement des solutions cloud au sein d'une entreprise demande-t-il des modes de gouvernance spécifiques ?*

Afin de répondre à notre question de recherche, nous baserons notre travail sur une étude qualitative de 35 grandes entreprises françaises. Nous avons exploré leur processus d'adoption des solutions *cloud*, le niveau d'intensité de leurs adoptions des solutions *cloud*, et enfin la manière dont ces entreprises gouvernent leurs solutions *cloud*.

Notre travail de recherche s'organise en trois parties : tout d'abord nous présentons une revue de la littérature relative à la gouvernance des TIC, au *cloud computing*, et aux modèles de maturité existant. Ensuite, nous préciserons la méthodologie de notre travail, puis présenterons les résultats sous deux grandes parties, que nous discuterons. Enfin, avant de conclure, nous indiquerons les limites de notre travail de recherche, les travaux de recherche futurs et nos contributions dans la littérature académique des Systèmes d'Informations.

# Revue de Littérature

## Section I : Gouvernance des TIC

### I. Définition des Systèmes d'Information

Plusieurs définitions coexistent pour les Systèmes d'Information (SI) depuis leur apparition en 1960. Van Der Aalst et Stahl (2011) définissent les SI, de manière très simple, en tant que systèmes gérant et traitant les informations d'une entreprise. Les SI d'une entreprise englobent plusieurs ressources : les individus, les données, les procédures, les *hardwares* et les *softwares*. Les individus d'un système d'information peuvent être internes (les salariés, les managers, les exécutifs) et externes (les clients, les fournisseurs) à l'entreprise. Les données, elles, constituent des informations vitales au bon fonctionnement de l'entreprise. En ce qui concerne les *hardwares* et les *softwares,* ces derniers sont responsables du support de l'information au sein des entreprises d'une part, et des réseaux et leurs constituants d'autre part. Ces cinq ressources sont indispensables pour permettre le bon fonctionnement du SI d'une entreprise.

Le SI vise dans un premier temps à rassembler les informations de l'entreprise, puis à les analyser et les stocker, pour finalement les communiquer à travers tous les départements de cette dernière. Un SI est un système multidimensionnel se constituant d'une dimension technologique (le SI fondé sur une architecture), organisationnelle (le SI soutenant les structures et processus organisationnels), et informationnelle (le SI produisant des résultats basés sur les données) (Reix et al. 2016).

### II. Définition des TIC

La définition des Technologies de l'Information et de la Communication (TIC) sur laquelle nous allons nous baser est présentée par Basque (2005, p.34) « *les technologies de l'information et de la communication renvoient à un ensemble de technologies fondées sur l'informatique, la microélectronique, les télécommunications (notamment les réseaux), le multimédia et l'audiovisuel, qui, lorsqu'elles sont combinées et interconnectées, permettent de rechercher, de stocker, de traiter et de transmettre des informations, sous forme de données de divers types (texte, son, images fixes, images vidéo, etc.), et permettent l'interactivité entre des personnes, et entre des personnes et des machines* ». La télécommunication et le calcul sont les bases des TIC afin de traiter et transmettre les informations sous différentes formes (textes, photos, messages vocal) (Turban et al. 2001).

Les TIC jouent un rôle très important dans le fonctionnement des entreprises, surtout durant cette ère digitale. *De facto*, le nombre d'entreprises basant leurs profits et leurs succès sur les TIC ne cesse d'augmenter, étant donné que l'adoption des TIC améliore les processus, renforce la collaboration entre les différentes parties-prenantes, et permet la création de nouveaux modèles d'affaires. En outre, plusieurs travaux de recherche ont prouvé l'avantage concurrentiel généré par l'adoption effective des TIC (Broadbent et Weill, 1997; ITL Education Solutions Limited, 2005; Lazic et al., 2011; Sharma, 2012; Urbach et al., 2013).

En revanche, la gouvernance des TIC est primordiale afin de bénéficier des avantages promis alors qu'une absence de gouvernance induit une stagnation de la croissance d'entreprise

(Weill et Ross, 2004; Sharma, 2012). Ceci nous amène à aborder le concept de la gouvernance afin de comprendre son rôle dans une entreprise.

## III. Définition de la gouvernance

La gouvernance représente le fait de distribuer le pouvoir, d'établir des politiques, de les mettre en œuvre et de les contrôler continuellement. Les gouvernements ainsi que les organisations (une entreprise, une administration, une association, un service public, une armée, etc.) ne peuvent fonctionner en l'absence de gouvernance, ce qui souligne son rôle primordial dans leur survie. Avant de se concentrer sur la gouvernance des entreprises, nous nous baserons sur la définition présentée par Alter (2002), représentant une entreprise en tant que la coordination de plusieurs systèmes établis pour atteindre les buts que chaque système isolé ne peut atteindre.

### 1. Niveaux de gouvernance

Plusieurs niveaux de gouvernance existent : la gouvernance d'entreprise, la gouvernance des SI, la gouvernance des TIC, etc. Nous allons consacrer la prochaine section afin de définir la gouvernance qui nous intéresse : celle des TIC.

### 2. Gouvernance des TIC

La gouvernance des TIC a été le centre d'attention d'un nombre important de travaux de recherche, où plusieurs définitions existent visant les différents aspects de la gouvernance. Ces dernières sont résumées dans le Tableau 1.

| **Définitions de la Gouvernance des TIC** | **Références** |
|---|---|
| Allocation des différents droits de prise de décisions et de responsabilités. | Sambamurthy et Zmud (1999); Weill et Woodham (2002); Simonson et Johnson (2006) |
| Maximisation de la valeur de l'entreprise par la mise en œuvre d'un alignement stratégique efficace. | Webb et al. (2006) |
| Mécanismes cherchant à réaliser la stratégie de l'entreprise. | Korac-Kakabadse et Kakabadse (2001); Van Grembergen et De Haes (2009) |
| Responsabilité du conseil d'administration et des cadres exécutifs. | Van Grembergen (2002); ITGI (2003); Parent et Reich (2009); Jewer et McKay (2012) |
| Allocation des droits de prise de décisions et la mise en œuvre de mécanismes afin d'effectuer ces décisions. | Luftman et Brier (1999); Sambamurthy et Zmud (2000); Peterson (2004); Weill (2004) |

Nous nous sommes basés sur la définition commune à Luftman et Brier (1999), Sambamurthy et Zmud (2000), Peterson (2004), et Weill (2004), selon laquelle la gouvernance des TIC se concentre sur l'allocation des différents droits de décisions par le biais de mécanismes (structures liées à la prise de décisions, processus *business*, et mécanismes relationnels). Cette définition englobe plusieurs aspects de la gouvernance qui nous intéressent dans notre travail de recherche.

La gouvernance des TIC s'avère être extrêmement importante pour le succès des entreprises. De nombreux travaux ont prouvé l'effet positif d'une gouvernance des TIC effective sur la performance de l'entreprise (Weill et Ross 2004), sa compétitivité (Rau 2004), l'alignement stratégique entre la direction des systèmes d'information (DSI) et les métiers (Van Grembergen et De Haes 2009), sa réduction des coûts et des risques (Parent et Reich 2009). Cependant, les entreprises doivent être conscientes de l'importance portée à la gouvernance effective de leurs TIC.

### 3. Domaines de la gouvernance des TIC

La gouvernance des TIC se compose de 5 domaines : l'alignement stratégique, la création de valeur (gouvernance stratégique), la gestion des risques, la gestion des ressources (gouvernance managériale) et la mesure de la performance (gouvernance opérationnelle) (Urbach et al., 2013; Buckby et al., 2008; Musson, 2008; Webb et al., 2006; De Haes et Van Grembergen, 2006; Meyer et al., 2003; ITGI, 2001). La gouvernance stratégique consiste à mettre en œuvre un alignement stratégique effectif entre la DSI et les métiers en créant de la valeur au sein de l'entreprise. Alors que la gouvernance managériale est responsable de la gestion des risques et des ressources de l'entreprise, la gouvernance opérationnelle s'occupe de mesurer sa performance. Par conséquent, une gouvernance effective des TIC consiste à adopter une gouvernance effective de ces cinq domaines.

### 4. Composantes de la gouvernance des TIC

Afin de gouverner effectivement les TIC d'une entreprise, il existe trois étapes primordiales à suivre. Premièrement, les entreprises doivent adresser des décisions primaires concernant les principes (*IT principles*), l'architecture (*architecture*), la stratégie de l'infrastructure (*infrastructure strategies*), les investissements (*investments*), la priorisation de leurs TIC (*IT prioritization*), ainsi que les décisions relatives aux besoins d'applications des métiers (*business application needs*) (Weill, 2004). Ces décisions doivent être allouées aux parties-prenantes appropriées prenant les bonnes décisions afin de garantir l'optimisation des bienfaits de l'entreprise. Traditionnellement, la DSI est considérée comme la plus apte à prendre des décisions concernant les TIC de l'entreprise. C'est surtout le cas pour les entreprises centralisées, contrôlées par leur DSI. Dans une entreprise décentralisée, le pouvoir est réparti entre les mains des directions métiers, ce qui signifie qu'ils seront plutôt les décideurs. Par ailleurs, après avoir analysé 256 entreprises, Weill et Ross (2004) concluent que les décisions sont prises par une de ces six parties : *business monarchy* (monarchie de métiers), *IT monarchy* (monarchie de DSI), *feudal* (féodale), *federal* (fédérale), *IT duopoly* (duopole de DSI) ou *anarchy* (anarchie). D'autres travaux de recherche se sont concentrés sur l'étude des décideurs les plus appropriés concernant les TIC. C'est le cas de Xue et al. (2008) qui affirment que sept archétypes de gouvernance sont possibles (*top management monarchy, top management IT duopoly, IT monarchy, administration monarchy, administration IT duopoly, professional monarchy, et professional IT duopoly*) ; ces derniers sont modérés par une gouvernance répartie sur deux étapes : l'initiation des décisions suivie par le développement des décisions.

Après avoir attribué chaque type de décisions aux décideurs les plus appropriés, l'implémentation des décisions se produit à l'aide des mécanismes de gouvernance des structures, des processus et des mécanismes relationnels. La gouvernance ne peut être effective qu'avec l'adoption de tels mécanismes.

Dans un premier temps, les structures sont définies comme les rôles et les responsabilités permettant la prise des décisions concernant les TIC (Peterson, 2004). La littérature académique a identifié un large nombre de structures efficientes pour la gouvernance des TIC. Parmi celles-ci, les rôles et responsabilités communiqués par le conseil d'administration et partagés par toute l'entreprise : la présence du DSI au sein du comité exécutif, le rapport régulier du PDG et du DSI au conseil d'administration, le locus du processus de prise de décisions (DSI centralisée, décentralisée, fédérale), la présence d'un comité de pilotage des TIC, d'un comité de stratégie des TIC, de comités de pratique de contrôle et de gouvernance (comité de révision d'architecture, comité de priorisation d'investissements, comité de révision de projets, comité pour la gestion de la qualité des données, centre d'excellence, bureau pour la gestion des services, conseil de risques) (Weill et Ross, 2005; Ali et Green, 2012; Vaswani, 2003 ; ITGI, 2003; De Haes et Van Grembergen, 2009; Bhattacharjya et Chang, 2006; Peterson, 2004; Héroux et Fortin, 2014). Bhattacharjya et Chang (2006) affirment que la présence de structures de gouvernance constitue la base pour des processus et des mécanismes relationnels plus développés.

A la suite de l'implémentation de structures pour la prise de décisions, il est impératif d'adopter des processus *business* de gouvernance. Ces processus sont définis comme des dispositifs pour la prise de décisions formelles assurant un comportement quotidien cohérent au sein de l'entreprise, par rapport aux politiques des TIC (Bowen et al. 2007). La littérature met en exergue plusieurs processus facilitant la gouvernance effective des TIC tels que les tableaux de bord prospectifs des TIC , la planification de systèmes d'informations stratégiques (e.g. planification de systèmes d'affaire – *Business System Planning* , facteurs clés de succès – *Critical Success Factors* , le modèle des forces concurrentiel de Porter – *Competitive forces model of Porter* , processus organisationnel de restructuration – B*usiness Process Reengineering approach* , chaines de valeur de Porter – *value chain models of Porter*), les référentiels de gouvernance (COBIT, ITIL, COSO), les accords aux niveaux de services (*Service Level Agreement*), ou encore le modèle d'alignement stratégique de Venkatraman et Henderson (1991) (De Haes et Van Grembergen, 2009; Bhattacharjya et Chang, 2006; Peterson, 2004; Ali et Green, 2012; ITGI, 2003; Hardy, 2003).

Les mécanismes relationnels, connus aussi sous le nom de mécanismes de communication, complètent les mécanismes de structures et processus pour l'adoption d'une gouvernance effective des TIC. Comme leur nom l'indique, ces mécanismes sont à la base de la communication interdépartementale au sein de l'entreprise. Elle doit être fortifiée et développée afin de pousser les départements à travailler ensemble et à aboutir à de meilleurs projets. Les travaux de recherche proposent un certain nombre de mécanismes relationnels: des connaissances partagées entre les métiers et la DSI, une participation active ainsi que des collaborations entre les différentes parties-prenantes, des récompenses et des primes de partenariat, une communication régulière entre les métiers et la DSI, une compréhension partagée des besoins des métiers et de la DSI, une rotation de postes et de formation transversales entre les métiers et la DSI, et enfin des campagnes de sensibilisation (Ali et Green, 2012; Weill et Ross, 2005; De Haes et Grembergen, 2005; Henderson et al., 1993; Broadbent, 1998; Luftman et Brier, 1999; Luftman, 2000; Reich et Benbasat, 2000; Callahan et Keyes, 2004; Peterson, 2004; Héroux et Fortin, 2014).

### 5. L'ère numérique et la gouvernance des TIC

Avec l'ère numérique, la gouvernance des TIC devient de plus en plus importante pour le succès des entreprises. Etant donné que les TIC sont disponibles au public, les concurrents d'une entreprise ont la possibilité d'imiter ses processus innovateurs, ce qui semble porter atteinte à l'avantage concurrentiel du marché. Afin de répondre à un environnement incertain et turbulent, les entreprises doivent développer une réactivité primordiale. Par conséquent, plusieurs travaux de recherche sensibilisent les entreprises à augmenter leur flexibilité, leurs adaptations au changement, ainsi que leur agilité stratégique afin d'affronter leurs concurrents (Reix et al., 2016; Brown et Grant, 2005; De Haes et Van Grembergen, 2004). Ainsi, tant que les entreprises s'adaptent facilement aux changements auxquels elles sont dorénavant affrontées, et gouvernent effectivement leurs TIC, elles auront la possibilité de bénéficier des avantages générés par les TIC, et surtout de ceux engendrés par les nouvelles technologies, tel le *cloud computing*.

# Section II : Le « *cloud computing* »

## I. L'évolution vers le *cloud*

Au cours des dernières décennies, plusieurs concepts ont conduit à l'émergence des solutions *cloud* en commençant par l'apparition des « mainframes » - ordinateurs centraux dans les années 60. C'est à partir de 1980 que les premiers ordinateurs personnels et réseaux en entreprise voient le jour. Durant les années 90, Internet apparaît et donne accès à la navigation sur le Web. Avec le développement d'Internet, de grandes entreprises telles que Google, Amazon, et Microsoft, débutent la construction de grands centres de données afin de permettre leur stockage et leur calcul. Par conséquent, le *cloud* commence son apparition d'une part en terme d'innovations technologiques, d'automatisation des centres de données, de haute performance, et de virtualisation (Boss et al., 2007), et d'autre part en terme de la naissance de « la perspective des services » (Vouk, 2008). L'émergence du *cloud* a stimulé une riche littérature, académique et professionnelle, concernant ses différentes caractéristiques : avantages, risques, prestation de services, impact du *cloud* en tant que « nouveau paradigme », etc. Le marché du *cloud* a beaucoup évolué depuis son apparition au début des années 2000 avec les solutions en ligne de CRM (gestion de la relation clientèle) fournis par salesforce.com. Amazon a pris le relais en 2002 avec ses offres « Amazon Web Services » et ses solutions cloud EC2 et S3 en 2006. Plusieurs fournisseurs ont rapidement imité Amazon avec la création de leurs propres solutions *cloud* (Google, IBM, Microsoft, HP).

## II. Définition et caractéristiques du *cloud*

Bien que le *cloud* ait été défini dans plusieurs travaux de recherche, sa définition la plus utilisée reste celle du « National Institute of Standards and Technology » aux Etats-Unis pour qui le *cloud* est « *l'accès via un réseau de télécommunications, à la demande et en libre-service, à des ressources informatiques partagées configurables* » (Mell et Grance, 2009, p. 1). Sur la base de cette définition, le *cloud* possède alors cinq caractéristiques clés : la disponibilité des ressources automatiques et en libre-service, l'élasticité, l'ouverture, la mutualisation et le paiement à l'usage. Grâce aux ressources en libre-service dont l'adaptation à la demande se fait automatiquement, les utilisateurs peuvent accéder à tous les services disponibles mondialement via Internet, et peuvent les utiliser automatiquement et immédiatement dès leurs demandes. En outre, le *cloud* est élastique, ce qui permet aux utilisateurs d'augmenter ou de diminuer la capacité dont ils ont besoin. Avec cela, le *cloud* est caractérisé par son ouverture aux différents services mis à disposition en ligne, qui sont standardisés, ce qui permet leur utilisation depuis un ordinateur, une tablette ou même un téléphone portable. Selon Mell et Grance (2009), la mutualisation des services *cloud* permet de combiner des ressources hétérogènes afin de servir plusieurs utilisateurs à qui les ressources sont attribuées immédiatement. Enfin, le *cloud* est connu pour son paiement à l'usage des ressources : l'utilisateur paie uniquement la quantité de services consommée.

## III. Composantes de l'écosystème du marché

L'écosystème du marché *cloud* représente un système complexe de composantes interdépendantes qui fonctionnent ensemble afin de fournir des solutions *cloud*. Les composantes principales pour le fonctionnement de l'écosystème *cloud* sont les fournisseurs *cloud* (CSP), les partenaires *cloud* (CSN), les utilisateurs *cloud* (CSU), les auditeurs, les parties-prenantes, et les comités de régulation (Martson et al., 2011; Schmidt et al., 2015). Les CSP, comme leur nom l'indique, fournissent des solutions *cloud* aux CSU. Les CSN sont une entité ou une organisation qui soutiennent la création des offres *cloud* par les CSP. Ce soutien se présente sous forme d'une intégration de logiciels, de fourniture de logiciels de migration de plate-forme, et de contrôle de logiciels. Lorsqu'un CSP fournit des solutions *cloud* à différents CSU, il peut avoir le soutien d'un CSN. Il peut aussi être fourni d'autres solutions *cloud* d'un autre CSP. Ceci montre la relation bidirectionnelle des différents composants de l'écosystème *cloud*. Les auditeurs, les parties-prenantes, et les comités de régulation font également partie de l'écosystème *cloud*, bien que leurs rôles soient moins dominants.

## IV. Les services *cloud*

Plusieurs services cloud sont proposés, dont l'Infrastructure en tant que service (IaaS), la plate-forme en tant que service (PaaS) et les logiciels en tant que service (SaaS). L'IaaS représente le niveau le plus bas qui consiste à offrir un accès à des machines virtuelles sur lesquelles les utilisateurs ont la possibilité d'installer leur système d'exploitation et leurs applications. Dans le mode IaaS, le fournisseur est responsable des couches de virtualisation, des plateformes matérielles, du réseau de stockage, de sauvegarde, « privé » ou externe et des partenaires externes. En revanche l'utilisateur est responsable de son système d'exploitation, des logiciels de base, des données et du code applicatif. La PaaS se trouve au-dessus de la couche d'IaaS, où l'utilisateur loue l'exploitation des serveurs sur lesquels les outils nécessaires sont déjà placés. Dans ce cas, l'utilisateur n'est responsable que de ses données et du code applicatif. Le troisième service cloud très utilisé est le SaaS, qui représente la troisième et dernière couche. Les utilisateurs de SaaS n'ont pas à se soucier de la manière dont les services sont fournis. Plusieurs exemples de services SaaS utilisés chaque jour existent, tels que les services de messageries, la bureautique virtuelle, les courriers électroniques, etc. Comme précisé dans la sous-section précédente, le fournisseur de SaaS peut être un utilisateur de service PaaS fourni par un autre fournisseur, qui lui-même peut être un utilisateur de service IaaS. Quelques exemples afin d'illustrer les différents services cloud : IaaS – Amazon EC2, Google Compute Engine ; PaaS – Google Application Engine, Microsoft Azure, Force.com ; SaaS – Salesforce.com, Google Apps, Microsoft Office 365.

## V. Les modèles de déploiement du *cloud*

Le *cloud* peut être public, privé, hybride, ou communautaire. Le *cloud* public est déployé par un fournisseur de *cloud* tiers, ouvert au public, et partagé mondialement par les différents utilisateurs. Le *cloud* privé, en revanche, est un *cloud* utilisé et manipulé par un seul organisme qui peut être hébergé en interne ou en externe. Le *cloud* hybride est un mélange de plusieurs modèles de *cloud* reliés entre eux et offrant les avantages des différents environnements. Enfin, le *cloud* communautaire est un *cloud* partagé par différents organismes ayant un intérêt commun, et généralement hébergé en externe.

## VI. Avantages et risques liés au *cloud*

D'ordre à la fois technique, économique, juridique ou applicatif, la littérature académique (Yang et Tate, 2009 ; Yang et Hsu, 2011 ; Zhang, et al., 2010 ; Oredo et Nijiha, 2014), comme professionnelle (CIGREF, 2013), met en évidence les grandes catégories de leviers et de freins à l'intégration de solutions *cloud*. En termes d'avantages, le *cloud*, quelque soit sa forme, est présenté comme extrêmement élastique et évolutif (Oredo et Njihia, 2014 ; He, 2011). Il permet d'accroître l'efficience, la flexibilité, l'innovation et l'agilité organisationnelles (Oredo et Njihia, 2014 ; He, 2011 ; Kim, 2009), mais permet également de réduire les coûts informatiques (*capital expenditure*, operating costs) en s'appuyant sur des offres commerciales adaptées (*pay per use*), et de bénéficier des dernières avancées technologiques (solutions les plus récentes et des *datacenters* puissants).

En termes d'inconvénients, la sécurité des données (à savoir l'accès et le piratage des données sensibles et personnelles ; Weiss, 2007 ; CIGREF, 2013), la réversibilité (contractuelles et techniques), la disponibilité des centres de données (congestion, bugs techniques, pannes de serveurs, cyber-attaques ; Gupta et al., 2013), la fiabilité, la performance des services *cloud*, et le coût apparaissent comme les principaux facteurs de risques. Le niveau élevé de leurs dépendances aux réseaux électriques, Internet (Yeboah-Boatang et Essandoh, 2014) et à l'informatique (Armbrust et al., 2010 ; Bojanova, 2013) interroge sur la crédibilité de solutions commercialisées et sur les garanties proposées par leurs fournisseurs (Leavitt, 2009 ; Srinivasan, 2013 ; Juels et Oprea, 2013).

## VII. Les contrats *cloud*

Les contrats *cloud* lient les utilisateurs à leurs fournisseurs. La signature de contrats *cloud* s'avère primordiale dès l'adoption de solutions *cloud*, même si celles-ci sont gratuites. Alors que ces solutions témoignent d'une rapide évolution des marchés, les contrats ne suivent pas la même vitesse. Les fournisseurs offrent à leurs utilisateurs des contrats standardisés, uniformes et rarement négociables afin qu'ils soient compatibles avec les lois prédominantes, ce qui facilite les transactions entre les deux parties. En outre, cette uniformité pousse les fournisseurs à se concentrer sur la satisfaction de leurs clients, ce qui leur permet de devenir plus compétitifs (Silalahi, 2011). Afin que les utilisateurs se sentent en sécurité de ne pas être les seuls à signer avec un CSP quelconque, ils bénéficient aussi de l'uniformité et de la standardisation de la majorité des contrats.

D'après la revue de la littérature, un contrat *cloud* possède plusieurs clauses, dont celle de responsabilité qui décrit les limites, l'exclusion et les solutions quand les garanties sont contrevenues, citant les indemnités possibles. De plus, les clauses de résistance, de disponibilité, de prestation et de niveau de services (« *Service Level Agreement* ») englobent des sujets différents tels que l'intégrité des données, la résistance de l'entreprise et sa continuité, les niveaux de service convenus, et la transparence des fournisseurs. Une clause essentielle pour la majorité des entreprises est la clause de confidentialité et du droit de contrôle, d'utilisation, et d'accès aux données des utilisateurs. En outre, la clause de réversibilité est largement évoquée, définissant les problèmes de réversibilité lors de la rupture du contrat par l'une des deux parties. Cette clause indique les étapes à suivre en lieu de rupture et déclare si le langage de programmation adopté pour les données des utilisateurs pourra être utilisé sur d'autres plates-formes. En outre, un grand nombre de clauses existe dans un contrat *cloud* afin de minimiser les risques possibles entre les deux parties.

## VIII. Gouverner les solutions *cloud*

### 1. L'impact des transformations opérées par le *cloud*

Plusieurs travaux de recherche évoquent les transformations engendrées par le *cloud*, liées à la façon dont les TIC sont manipulées dans l'entreprise (Carr, 2008 ; Zhang et al., 2010 ; Venters et Whitley, 2012). En revanche, les transformations organisationnelles ne s'avèrent pas facilement implémentées, selon Carr (2008) qui note que l'un des obstacles les plus communs aux entreprises souhaitant adopter des solutions *cloud* n'est pas lié aux aspects technologiques mais plutôt à l'attitude de l'entreprise envers l'implémentation de telles solutions. Martson et al. (2011) affirment que l'émergence du *cloud* change la structure informatique de l'entreprise où diverses problématiques intra-organisationnelles devraient être abordées, telles que le changement culturel, la façon d'adresser ce changement, et la façon de convaincre les salariés d'accepter ce changement. D'autres travaux de recherche mentionnent les problématiques de savoir-faire limité, où les entreprises peuvent avoir du mal à s'ajuster aux changements, principalement durant les premières phases de son adoption (Wang et Ramiller, 2009). En outre, le *cloud* complique la gouvernance des TIC dans l'entreprise, surtout par rapport aux décisions prises par les différentes parties-prenantes. Ces décisions doivent envisager les problématiques liées aux solutions *cloud*, telles que la réversibilité, l'interopérabilité, la reprise après sinistre, la gestion partagée, ou encore l'interdépendance sur les fournisseurs (Hsu, 2012). Par conséquent, certains pointent l'importance d'établir des politiques ainsi que des normes dans les premières phases de l'adoption, afin de maintenir une gouvernance effective des TIC (Hsu, 2012 ; Martson et al., 2011). En plus des politiques et des normes, il est impératif de créer une stratégie pour gérer les problématiques liées aux solutions *cloud*. Les travaux de recherche antérieurs conseillent aux grandes entreprises de construire leurs propres stratégies *cloud* en garantissant que les objectifs des directions métiers soient alignés à ceux de la DSI (Martson et al., 2011).

### 2. L'impact sur les compétences des DSI

L'un des nombreux changements engendrés par l'apparition du *cloud* est le besoin impératif de nouvelles compétences. En effet, le manque de compétences spécifiques au *cloud* a été cité comme étant un inconvénient majeur (Rajendran, 2013 ; Dutta et al., 2013 ; Kim, 2009). Selon une enquête menée par Portio Research en 2009, 56% des DSI Européennes interviewées (196 DSI sur 350) ne possèdent pas les connaissances requises ni les compétences nécessaires pour pouvoir mettre en place des solutions *cloud* sophistiquées (Flechaux, 2009). Comme mentionné antérieurement, avec l'adoption des solutions *cloud*, la notion de contrat devient plus importante. Par conséquent, les employés doivent accroître leurs compétences en matière de contrat, afin de pouvoir les lire et les analyser méticuleusement et ainsi éviter toute confusion, mal-interprétation ou incompréhension. Le problème lié au manque de compétences dans ce domaine soulève des questions primordiales relatives à la gouvernance des TIC de l'entreprise afin que celle-ci reste compétitive. Les différents départements, et principalement les DSI, sont conseillés d'assister à des sessions de formation afin de développer leurs compétences, ce qui diminuera le niveau d'anxiété des employés de la DSI et réinstaurera leur confiance en leurs compétences. Ceci est évoqué par Morgan et Conboy (2013) qui soulignent le haut niveau de stress éprouvé par les employés de la DSI qui craignent que leurs compétences deviennent obsolètes. De plus, l'arrivée du cloud au sein des entreprises les pousse à aligner les objectifs des directions métiers avec ceux de la DSI (Weill et Ross, 2004). Etant donné que les solutions cloud représentent de nouvelles ressources informatiques, elles exigent de nouvelles compétences ainsi que des nouvelles structures de gouvernance afin d'aligner les objectifs au sein de l'entreprise (Prasad et Green, 2015).

### 3. Nouveaux mécanismes de gouvernance

Les travaux de recherche menés antérieurement ont montré que les mécanismes de gouvernance présents au sein d'une entreprise ne sont pas suffisants pour gouverner les solutions *cloud*. Cela est dû aux problématiques citées dans la section précédente (Martson et al., 2011 ; Joha et Janssen, 2012 ; Prasad et al., 2014). Il est donc conseillé d'implémenter de nouveaux mécanismes adaptés aux solutions *cloud* afin de pouvoir bénéficier de tous les avantages qu'elles génèrent. Toutefois, les travaux de recherche par rapport aux mécanismes de gouvernance spécifiques au cloud demeurent rares. Prasad et al. (2014) proposent de nouvelles structures de gouvernance telles qu'un *Chief Cloud Officer* (coordination des solutions cloud), un Comité de Gestion du Cloud (gestion des solutions cloud dès leurs expansions dans l'entreprise), un Service de Facilitation du Cloud (centre opérationnel gérant les bases de données des fournisseurs) et un Centre Relationnel du Cloud (gestion de la relation entre les fournisseurs et les employés). D'autres auteurs (Joha et Janssen, 2012) proposent également d'autres structures de gouvernance : capabilités en gestion de relation, gestion de la sécurité de data, gestion des risques, gestion du réseau, approvisionnement des solutions cloud, etc. Ces travaux de recherche mettent en lumière le rôle du Directeur des Systèmes d'Information qui a désormais besoin d'être accompagnés durant ces transformations digitales par d'autres structures, d'où l'émergence du *Chief Digital Officer* (CDO). Ce dernier possède des compétences informatiques ainsi que des compétences métiers (Horlacher et Hess, 2016).

En revanche, les travaux antérieurs n'ont pas  mis en évidence les mécanismes de processus et relationnels spécifiques pour l'adoption des solutions *cloud*.

### 4. Modèles existant de gouvernance du *cloud*

Rares sont les travaux ayant tenté d'adresser la question de gouvernance du *cloud*. Que quelques auteurs se sont intéressés à la conception d'un modèle spécifique au *cloud*, pourtant sans se concentrer sur les mécanismes de gouvernance. En se focalisant sur les aspects généraux du *cloud*, le modèle présenté par Guo et al. (2010), par exemple, est divisé en trois sous-parties : la partie politique du cloud, la partie opérationnelle, et la partie managériale. Leur modèle néglige la partie stratégique accompagnant l'adoption des solutions *cloud*, ainsi que la partie de restructuration de l'entreprise mentionnant les différents rôles, structures et responsabilités nécessaires pour une gouvernance effective. Un autre modèle de gouvernance du *cloud* est le modèle présenté par Hsu (2012). Ce modèle consiste à définir des politiques et des principes clairs pour créer une stratégie de gouvernance effective accompagné d'un plan de gestion. En revanche, ces modèles n'adressent pas tous les aspects du *cloud* ce qui semble rédhibitoire pour une gouvernance effective.

A ce jour, les modèles de gouvernance matures du *cloud* sont peu ou prou présents dans la littérature. Etant donné que le *cloud* est considéré comme innovation technologique, il fait partie des TIC de l'entreprise. Ainsi, nous nous demandons si l'implémentation des solutions cloud peut être gouvernée par la gouvernance des TIC existante de l'entreprise. Afin d'explorer la gouvernance des solutions *cloud*, il serait intéressant d'étudier le lien possible entre cette gouvernance et le degré d'intensité d'adoption des solutions *cloud*, et ceci via l'exploration des modèles de maturité présents dans la littérature.

# Section III : Modèles de maturité de gouvernance

## I. Définition du modèle de maturité

Un modèle est représenté comme étant une description d'environnement afin de comprendre ce qui se passe au sein de cet environnement (Mettler et Rohner, 2009). En outre, la maturité est expliquée par Simpson et Weiner (1989) comme étant l'état prêt, complet et « parfait ». Afin d'atteindre cet état « parfait », les entreprises doivent faire évoluer leur état actuel (généralement, l'état Ad Hoc) jusqu'à l'état requis. Les modèles de maturité antérieurement développés sont composés de divers niveaux de maturité, ayant pour objectifs d'aider les entreprises dans leur évolution d'un état au suivant afin d'atteindre l'état « parfait » (Lahrmann et al., 2011).

## II. Modèles de maturité existant

Il existe plusieurs travaux ayant adressé les méthodes d'évaluation des entreprises ainsi que les *frameworks* de gouvernance informatique, tels que le *Control Objectives for Information and related Technology* (COBIT), le *Capability Maturity Model* (CMM), le *Capability Maturity Model Integration* (CMMI), et l'*IT Capability Maturity Framework* (IT-CMF). En revanche, rares sont les travaux académiques ayant tenté d'adresser les modèles de maturité de *cloud*. L'Open Data Center Alliance (ODCA), un consortium visant à guider les entreprises dans la transformation numérique liée au *cloud*, a identifié l'importance d'un modèle de maturité des solutions *cloud* afin de soutenir le développement d'une stratégie *cloud*, de souligner les domaines de gouvernance à développer impérativement, et de bénéficier des avantages promis par l'adoption de telles solutions. Ce consortium a développé un « *Cloud Maturity Model* » en se basant sur le modèle de maturité CMMI et en mesurant les capabilités *cloud* sur cinq niveaux de maturité. Suite à l'absence de model de maturité pour les solutions *cloud* dans la littérature académique, nous allons nous baser sur le modèle (professionnel) proposé par l'ODCA (2013).

## III. Le « Cloud Maturity Model® »

Le « *Cloud Maturity Model* » (ODCA, 2013) identifie deux perspectives de maturité : la première concerne le côté business et la seconde le côté informatique. Chaque perspective possède 4 domaines. La partie business englobe la stratégie d'entreprise, les compétences, la gouvernance (côté business), ainsi que les projets, portfolios, et services. Le côté informatique, quant à lui, comprend l'administration, les opérations et la gouvernance (côté informatique), l'information, l'architecture, et l'infrastructure. Ce modèle représente la maturité des solutions cloud sur cinq niveaux : CMM1 (niveau initial d'adoption des solutions cloud caractérisé par la présence d'infrastructures (et du *legacy*) au sein de l'entreprise, la phase d'analyse de la transformation digitale et de la migration vers le *cloud*), CMM2 (définition, transformation, et mise à jour des processus, migration vers un *cloud* privé et potentiellement vers un *cloud* publique), CMM3 (toutes les parties-prenantes se sont mises d'accord pour la migration vers le cloud public, introduction d'outils sophistiqués pour la gestion de risques, émergence du PaaS privé), CMM4 (implémentation de mécanismes de gouvernance afin d'évaluer la maturité des solutions *cloud*, focus sur les besoins des métiers), CMM5 (dernier niveau de maturité, implémentation optimale des solutions *cloud*). Le but du modèle est d'évaluer la maturité de chaque domaine de l'entreprise et ce à l'aide d'un questionnaire proposé par le consortium afin de faciliter l'évaluation (ODCA, 2013). Etant donné que ce modèle adresse le côté métiers ainsi que le côté DSI, il s’avère intéressant de se baser sur les différents aspects présentés par ODCA (2013).

# Design de Recherche

## I. Méthodologie qualitative

Le taux d’adoption des solutions *cloud* ne cesse d’augmenter, ce qui pousse les travaux de recherche à s’intéresser mondialement à ce sujet. Bien que les outils quantitatifs, comme les questionnaires, forment une méthode convenable pour étudier la gouvernance des solutions *cloud* dans les grandes entreprises françaises, les outils qualitatifs, au travers d’entretiens avec les employés les plus adéquats, seront capables de révéler des détails plus approfondis, bien que négligés par les questionnaires. Dans notre cas de recherche, une approche qualitative semble être la plus appropriée pour plusieurs raisons. Premièrement, nous sommes intéressés par les différentes perceptions et opinions des entreprises par rapport à leurs expériences avec les solutions *cloud*. La méthodologie qualitative est utile lors de la définition des attitudes et perceptions tout en réduisant les barrières entre le chercheur et les participants (Stake, 1995). En outre, elle nous aide à mieux comprendre les interprétations des participants concernant le sujet du *cloud* dans les entreprises françaises. Enfin, une telle méthodologie nous est nécessaire afin de construire, d’une manière inductive, un *framework* basé sur la façon dont les entreprises françaises gouvernent leurs solutions *cloud*.

## II. Epistémologie

Après avoir exploré la méthodologie la plus adaptée à notre travail, nous nous sommes penchés vers la recherche d’une épistémologie qui nous aidera à répondre à notre question de recherche. Hirschheim (1992) affirme que chaque travail de recherche se base sur des suppositions philosophiques de ce qui constitue la recherche “validée” et la façon dont la connaissance est obtenue durant une étude donnée. En ayant à l’esprit l’analyse des perceptions et des opinions de nos participants qu’il nous faudra mener, nous nous sommes penchés vers l’interprétativisme ; une épistémologie pour laquelle la réalité est formée par des valeurs sociales, politiques, culturelles, économiques, ethniques, et de genre.

## III. Méthodes

Ayant pour objectif de répondre à notre question de recherche : *Le déploiement des solutions cloud au sein d’une entreprise demande-t-il des modes de gouvernance spécifiques ?* Après nous avoir mis d’accord sur la méthodologie et l’épistémologie les plus adéquates, nous avons décidé de nous baser sur des entretiens et des documents complémentaires (en tant que ressources secondaires). Le Tableau 1 détaille les méthodes adoptées durant notre travail de recherche.

**Tableau 31: Description détaillée des méthodes adoptées**

| | | | | |
|---|---|---|---|---|
| **Entretiens** | Phase I | Contacts des participants potentiels | Intervalle | Août 2015 à janvier 2016 |
| | | Collecte de données | Type | Entretiens semi-directifs |
| | | | Intervalle | Novembre 2015 à avril 2016 |
| | | Analyse des données | Méthode | Codage et traitement analytique par Nvivo |

| | | | | |
|---|---|---|---|---|
| | | | Intervalle | Août 2016 à octobre 2016 |
| | Phase II | Contact des Participants | Intervalle | Novembre 2016 à janvier 2016 |
| | | Collecte de données | Type | Entretiens directifs |
| | | | Intervalle | Janvier 2017 à mars 2017 |
| | | Analyse des données | Méthode | Analyse du niveau d'intensité d'adoption des solutions *cloud* |
| | | | Intervalle | Avril 2017 à mai 2017 |
| **Documents Complémentaires** | | Collecte de données | Type | - Emails informatifs<br>- Référence de sites web<br>- Documents montrant différents processus, missions, etc. |
| | | | Intervalle | Durant et après la Phase I des entretiens |

# IV. Entretiens – Phase I

## 1. Collecte des données

Afin d'explorer la gouvernance des solutions *cloud* par les entreprises françaises, nous avons mené en premier temps des entretiens semi-directifs avec des employés métiers et de la DSI, de grandes entreprises, publiques et privées. Les 35 entretiens ont duré entre 35 et 88 minutes (une durée moyenne de 59,5 minutes). Les travaux antérieurs ont prouvé que l'implémentation des solutions *cloud* dans les grandes entreprises relève plus de défis (Winkler et al., 2014 ; Venters et Whitley, 2012), ce qui nous a donc poussé à nous concentrer sur les grandes entreprises françaises, entre novembre 2015 et avril 2016. Les thèmes abordés renvoient aux objectifs qui ont présidé i) au choix de recourir au *cloud* en termes de levier, de performance à atteindre et des avantages perçus ; et ii) à la pratique en termes de mise en œuvre (gouvernance des TIC et des solutions *cloud*). Ces entretiens ont été enregistrés et intégralement retranscrits afin d'engager une analyse de discours via le logiciel Nvivo, version 11,0. En outre, après avoir analysé 560 dissertations de thèses, Marson (2010) a conclu que la moyenne des corpus dans les travaux académiques pour une approche qualitative était de 31 entretiens. Par conséquent, nous étions satisfaits par l'intégralité de 35 entretiens menés. La description détaillée de ces derniers est représenté dans le Tableau 2.

**Tableau 32: Description détaillée de nos participants**

| **Ref.** | **Domaine** | **Acteur interrogé** | **Industrie** | **Secteur** | **Mode des décisions** | **Services adoptés** | **Durée d'entretien s (min)** |
|---|---|---|---|---|---|---|---|
| B.1 | Business | PDG | Centre de Recherche | Publique | Décentralisé | IaaS, SaaS | 49 |
| IT.1 | IT | DSI | Assurance (Retraite) | Privé | Centralisé | PaaS, SaaS | 55 |
| IT.2 | IT | DSI | Transport | Privé | Décentralisé | IaaS, SaaS | 67 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IT.3 | IT | Manager Senior projets IT | Transport | Privé | Centralisé | IaaS, PaaS, SaaS | 71 |
| IT.4 | IT | DSI | Grande distribution | Privé | Centralisé | IaaS, SaaS | 61 |
| IT.5 | IT | Manager Senior projets IT | Assurance | Privé | Décentralisé | IaaS, SaaS | 62 |
| IT.6 | IT | DSI | Banque | Privé | Centralisé | IaaS, PaaS, SaaS | 63 |
| IT.7 | IT | DSI | Média | Privé | Décentralisé | IaaS, SaaS | 81 |
| IT.8 | IT | Manager Senior projets Cloud Computing | Assurance | Privé | Décentralisé | IaaS, SaaS | 58 |
| IT.9 | IT | DSI | Assurance (Familiale) | Publique | Centralisé | IaaS, SaaS | 58 |
| IT.10 | IT | DSI | Assurance (Retraite) | Publique | Centralisé | IaaS, PaaS, SaaS | 62 |
| IT.11 | IT | DSI | Fournisseur d'énergie | Privé | Décentralisé | IaaS, SaaS | 88 |
| IT.12 | IT | DSI | Fournisseur d'énergie | Privé | Décentralisé | IaaS, SaaS | 53 |
| IT.13 | IT | DSI | Fabrication | Privé | Centralisé | IaaS, PaaS, SaaS | 62 |
| B.2 | Business | PDG | Fabrication | Privé | Décentralisé | SaaS | 42 |
| B.3 | Business | PDG | Déclaration Sociales | Publique | Décentralisé | IaaS, SaaS | 35 |
| IT.14 | IT | Manager Senior projets IT | Fournisseurs d'énergie | Privé | Décentralisé | IaaS, SaaS | 85 |
| B.4 | Business | Manager Senior projets | Santé | Privé | Centralisé | IaaS, SaaS | 52 |
| B.5 | Business | PDG | Production | Privé | Décentralisé | IaaS, SaaS | 48 |
| IT.15 | IT | DSI | Poste | Privé | Décentralisé | IaaS, SaaS | 64 |
| B.6 | Business | Manager projets IT Cloud Computing | Fournisseurs d'énergie | Privé | Décentralisé | IaaS, SaaS | 68 |
| B.7 | Business | PDG | Production | Privé | Décentralisé | IaaS, SaaS | 64 |
| B.8 | Business | PDG | Média | Privé | Centralisé | IaaS, PaaS, SaaS | 70 |
| IT.16 | IT | DSI | Télécommunication | Privé | Décentralisé | IaaS, SaaS | 75 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IT.17 | IT | DSI | Transmission d'énergie | Privé | Décentralisé | IaaS, SaaS | 42 |
| IT.18 | IT | DSI | Production | Privé | Décentralisé | IaaS, SaaS | 45 |
| IT.19 | IT | Assistante de direction d'états interministériels (DSI) | Services du Premier Ministre | Publique | Centralisé | IaaS, SaaS | 47 |
| IT.20 | IT | DSI | Action Publiques | Publique | Centralisé | IaaS, SaaS | 48 |
| IT.21 | IT | DSI | Finances | Publique | Centralisé | IaaS, SaaS | 65 |
| B.9 | Business | PDG | Grande Distribution | Privé | Décentralisé | IaaS, SaaS | 57 |
| IT.22 | IT | Manager Senior projets IT | Banque | Privé | Centralisé | IaaS, SaaS | 78 |
| B.10 | Business | PDG | Production | Privé | Décentralisé | IaaS, SaaS | 49 |
| IT.23 | IT | DSI | Enseignement Supérieur | Public | Décentralisé | IaaS, PaaS, SaaS | 59 |
| B.11 | Business | PDG | Production | Privé | Centralisé | IaaS, SaaS | 45 |
| IT.24 | IT | Manager Senior projets IT | High Tech | Privé | Décentralisé | IaaS, SaaS | 54 |

### 2. Analyse des données

Les entretiens intégralement retranscrits et les prises de notes effectuées lors de chaque session ont été analysés à l'aide du logiciel Nvivo. Sur les recommandations d'Elliot et Timulak (2005), la phase d'analyse a été guidée par une perspective critique, auto-réfléchissante, et sceptique, durant laquelle nous avons commencé par diviser nos données en « unités de sens distinctives ». Le premier tour de codage a identifié plusieurs codes auxquels nous avons attribué différents fragments de textes. Les catégories de codes ont été influencées par les résultats de notre revue de la littérature approfondie. Par exemple, les opportunités et les risques de l'adoption des solutions cloud forment une catégorie à laquelle plusieurs sous-catégories ont été créées, comme suggéré par Elliot et Timulak (2005). Afin d'illustrer les catégories, prenons le verbatim du participant IT.2 « *l'adoption des solutions cloud pour nos différents usages nous effraie un peu, surtout à cause des questions de réversibilité. Ne pas avoir une certitude de récupérer toutes nos données à la fin de nos contrats avec les fournisseurs freine notre adoption* ». Ce verbatim a tout d'abord été codé sous la catégorie « *Barrières du cloud* » et durant le deuxième tour de codage a été codé sous la catégorie « *Réversibilité* ». Il est important de noter que même si les catégories ont émergé de manière inductive, notre question de recherche et notre revue de la littérature ont influencé la thématique de ce processus inductif.

# V. Entretiens – Phase II

## 1. Collection des données

Les résultats de l'analyse des données du premier tour d'entretiens ont conduit à la réalisation d'un second tour d'entretiens ayant pour objectif l'étude du lien potentiel entre l'adoption d'une gouvernance des TIC effective et le niveau d'intensité d'adoption des solutions *cloud* (niveau de maturité) au sein des grandes entreprises. Ce second tour a été réalisé avec les mêmes participants mais suivant un mode directif. Grâce aux connaissances avancées de nos participants, diplômés d'écoles d'ingénieurs ou de commerce prestigieuses, et leurs expériences dans leurs entreprises, nous les avons jugés capables d'évaluer le niveau de maturité de leurs solutions *cloud*. Durant ce second tour d'entretiens, nous nous sommes basé sur le modèle de maturité proposé par ODCA (2013) et nous avons donc posé 18 questions (ODCA, 2013), concernant le niveau d'intensité d'adoption, auxquelles les participants ont attribué une réponse unique pour chacune.

## 2. Analyse des données

ODCA (2013) pointe que la maturité des solutions *cloud* dans une entreprise est évaluée selon 8 domaines. Par conséquent, nous avons commencé l'analyse des résultats en calculant la moyenne de chaque domaine, pour enfin calculer la moyenne totale de chaque entreprise (ODCA, 2013). Le calcul de la maturité de chaque domaine a pour objectif de guider les entreprises à évaluer et améliorer le(s) domaine(s) en nécessité. Après avoir calculé la moyenne totale de chaque entreprise, nous les avons classées en fonction du niveau auquel elles appartiennent (CMM1, CMM2, CMM3, CMM4, ou CMM5).

# VI. Documents complémentaires

Comme mentionné antérieurement, nous avons eu recourt à des documents complémentaires afin de fortifier nos analyses. Nous avons tout d'abord utilisé des données reçues via des échanges d'emails, où les participants nous ont communiqué des informations concernant leur adoption des solutions *cloud*. De même, durant les entretiens, certains participants nous ont fournis des documents annexes, tels que la liste de leurs processus, leurs missions, leurs projets futurs, etc. Nous avons aussi basé notre analyse sur des articles en ligne, ainsi que sur les sites internet de quelques entreprises.

# Analyse des Résultats

## Partie I

### I. Impact des solutions *cloud*

L'analyse de nos entretiens a abouti à l'observation de plusieurs transformations induites de l'émergence des solutions *cloud*, notamment le rôle de la DSI. Tandis que la DSI visait à livrer ses projets, le plus rapidement possible et tout en restant dans la limite du budget, la digitalisation souligne l'importance de mettre les besoins des métiers en avant, les poussant à s'orienter dans ce sens. Pendant que les entreprises témoignent d'une transition du rôle de leurs DSI par la digitalisation, cette dernière engendre une transition de pouvoir de la DSI vers les directions métiers. Les DSI évoluent d'un rôle prescriptif vers un rôle proactif (IT.17, IT.16, IT.8, IT.14), fournissant de « *meilleurs stratégies et solutions* » (IT.17). La digitalisation des entreprises transforme aussi les profils des DSI pour le développement de nouvelles compétences requises durant l'adoption des solutions *cloud*. On note également d'une part l'influence sur le système d'éducation français, où « *les grandes écoles ou même les universités publiques doivent adapter leur cours et leurs méthodologies à la transformation digitale atteinte aujourd'hui* » (IT.16), et d'autre part que les syndicats doivent être formés aux changements générés par le *cloud*. L'ubiquité des solutions *cloud* pousse les employés au télétravail ce qui ne rentre pas dans les caractéristiques de la loi du travail en France. Par conséquent, il est aussi impératif « *de former et sensibiliser les syndicats par rapport à cette évolution* » (IT.16). Nos analyses ont aussi mis en valeur certaines transformations internes, comme la transformation vers des « *processus automatisés* » (IT.14), la transition vers « *une infrastructure ouverte par l'adoption des solutions PaaS et IaaS* » (IT.15), l'implémentation de « *nouveaux modèles d'affaires et nouvelles méthodologies* » (IT.12), et finalement « *la transition d'une vérification de sécurité technologique vers une contractuelle* » (IT.11). Etant donné que « *les contrats cloud sont signés pour une longue durée* » (IT.16), les entreprises ont noté « *l'ajout des fournisseurs cloud fiables* » (IT.9) à leur liste de partie-prenantes. Enfin, les solutions *cloud* engendrent des changements dans la « *data privacy* » des entreprises où ce concept devient crucial, essentiel et primordial.

### II. « Shadow IT »

Les analyses des entretiens nous ont permis d'identifier quelques entreprises qui ne possèdent pas des activités de « *shadow IT* » où leurs DSI sont centralisées et leurs budgets sont extrêmement contrôlés. Néanmoins, la majorité des entreprises affrontent plusieurs cas de « *shadow IT* » surtout dû aux délais serrés des métiers, nécessitant des solutions le plus rapidement possible.

### III. Motivations

Nos entretiens soulèvent trois déclencheurs de l'adoption des solutions *cloud*. Alors que certains affirment qu'ils se sont penchés vers le *cloud* afin de rester dans le marché très compétitif (IT.16, IT.7, IT.15, IT.24, IT.8), d'autre s'appuient sur le côté innovant de ces solutions (IT.12, IT.3, B.9, IT.14, IT.11, IT.18, IT.15, B.6, B.10, IT.23, B.8, IT.17, IT.9, IT.10, IT.20, IT.19, IT.2). Enfin, une grande partie des entreprises évoquent les bénéfices économiques du *cloud* et surtout leurs réductions des coûts, ce qui les a motivées vers son adoption (IT.22, B.11, IT.15, IT.2, IT.4, B.4, IT.21, IT.13, B.8, IT.6, IT.17, B.5, IT.1, B.1, B.2, B.7, B.3).

## IV. Bienfaits et Risques

De manière similaire à la littérature académique, les entreprises soulignent les bienfaits suivants générés par l'adoption des solutions cloud : les bienfaits économiques (le paiement à l'usage, les coûts bas, et la consommation électrique basse), la scalabilité (structure *cloud* flexible), l'agilité (des cycles de développement plus courts, plus de communication, développement de solutions plus rapidement), la performance (structure agile plus performante), et l'ubiquité (mobilité des solutions). Tandis que les travaux antérieurs affirment que la standardisation des solutions *cloud* est un frein pour les entreprises, nos entretiens rejettent cet argument en affirmant que cette standardisation les sécurise, ce dont ils sont satisfaits.

En ce qui concerne les risques perçus par nos participants, l'analyse des résultats a identifié : les risques de sécurité (données critiques, attaques internes et externes, perte de données), la réversibilité (clause de réversibilité, transition vers d'autres fournisseurs), la conformité (localisation des données en dehors de la zone Européenne, suivi des lois conformes à celles de la France), et les risques sociétaux (licenciements d'employés). En outre, un nouvel élément, qui n'a pas été mentionné dans la littérature académique, ressort de nos analyses : la dépendance sur les fournisseurs. Les solutions fournies aux entreprises peuvent cesser d'exister à la fin de leurs contrats, voire durant la durée du contrat, ce qui rend ces entreprises dépendantes de leurs fournisseurs, les laissant ainsi dans une position vulnérable.

## V. Gouvernance des solutions *cloud*

### 1. Décisions « *cloud* »

L'analyse de nos données souligne d'importantes questions que nos participants ont adressées durant la phase *Ad Hoc* d'adoption des solutions *cloud*. Pendant que certaines entreprises se renseignent sur l'utilité du *cloud*, d'autres discutent des diverses étapes nécessaires pour la transition vers le *cloud*. En outre, les participants mentionnent à l'unanimité l'importance de se décider sur les modèles de déploiement ainsi que les services *cloud* à adopter. De plus, plusieurs participants se sont concentrés sur les décisions en lien avec les bienfaits économiques, les risques de sécurité, la localisation de leurs données, et le besoin d'obtenir de nouvelles compétences. En revanche, seuls quelques-uns pointent des discussions récurrentes concernant les problématiques issues des contrats *cloud*, les transformations techniques et politiques, ainsi que leurs relations avec les fournisseurs et leurs clients.

### 2. Prise de décisions « *cloud* »

Selon l'analyse des entretiens, plusieurs décideurs différents ont été mentionnés, ce qui montre que l'adoption des solutions *cloud* influence la prise de décisions de nos participants. D'une part, les entreprises centralisées attribuent la responsabilité des décisions à leurs DSI, et d'autre part, le reste des entreprises s'assurent que les différents départements prennent part au processus de prise de décisions (via leur collaboration). En revanche, malgré le fait qu'une collaboration soit présente, nos participants affirment que l'arbitrage se fait par la DSI (B.1, IT.5, IT.7, IT.8, etc.), le conseil d'administration (IT.3), le département des finances (IT.22), ou même parfois par l'Etat (IT.19).

#### 3. Mécanismes de gouvernance

Des mécanismes additionnels de gouvernance (structures, processus, relationnel) s'imposent afin de gouverner effectivement les solutions *cloud*. Selon nos participants, certains mécanismes étaient déjà implémentés au sein de leurs entreprises, mais ils ont eu recourt à de nouveaux mécanismes spécifiques pour le *cloud*.

Les structures qui ressortent de nos analyses sont les suivantes : la présence d'un *Chief Digital Officer* (CDO) ; d'un conseil d'architecture ; d'un *Chief Data Privacy Officer* ; d'un *Chief Security Officer* ; d'un comité technique de l'architecture ; d'un comité de stratégie dévoué au *cloud* ; d'un comité d'achats ; de comités technique et juridique ; d'un *Chief Exchange and Digital Officer* ; d'un comité de la gestion des données ; d'un *Scrum Master* ; d'un expert de *Data Mining* ; le rapport des DSI et du PDG au conseil d'administration.

En ce qui concerne les processus mentionnés, nos analyses n'en relèvent que quelques-uns : des processus spécifiques aux entreprises, les *frameworks* de gouvernance des TIC dévoué aux questions liées au *cloud*, les méthodologies agiles, les tableaux de bord.

En outre, plusieurs mécanismes relationnels additionnels, qui ont permis à nos participants de mieux gouverner leurs solutions *cloud*, ont été mentionnés : de la communication et des relations plus proches entre les directions métiers et la DSI, une rotation de postes et de formations transversales entre les métiers et la DSI, des campagnes de sensibilisation, des connaissances partagées par les métiers et la DSI, des récompenses et des primes de partenariat, ou encore des relations développées entre l'entreprise et ses fournisseurs.

## VI. Contrats « *cloud* »

Nos résultats mettent en valeur l'importance des contrats *cloud* pour nos participants, surtout dans le cas des entreprises publiques. Trois clauses primordiales ont été mentionnées : la clause de réversibilité, de confidentialité et de l'accord du niveau de services (*SLA*). Certains participants affirment qu'avant la signature des contrats, ils « *tournent la page vers la clause de réversibilité, afin de vérifier les termes* » (IT.15). De plus, la clause de confidentialité devrait être bien rédigée afin de garantir la protection et la localisation de leurs données dans la zone Européenne (IT.9, IT.11, IT.12, B.4, IT.15, IT.16, IT.19, IT.20, B.10, IT.23). Enfin, les participants s'attendent au niveau de service promis lors de l'accord initial.

# Partie II

## I. Classification de groupes

Afin d'évaluer les niveaux d'intensité des entreprises (i.e. leurs maturités en termes d'adoption de solutions *cloud*), nous nous sommes basés sur la classification proposée par ODCA (2013). Nous avons donc classé chaque entreprise selon le niveau de maturité correspondant, en se basant sur la moyenne des 18 questions posées. Nous rappelons que les 18 questions sont réparties en 8 domaines : la stratégie d'entreprise (Q1-Q3) ; l'entreprise et les compétences (Q4-Q6) ; la gouvernance (côté business) (Q7-Q10) ; les projets, portfolios, et services (Q11-Q12); l'administration, les opérations et la gouvernance (côté informatique)

(Q13) ; l'information (Q14); l'architecture (Q15-Q17) ; et l'infrastructure (Q18). Les 18 questions posées sont les suivantes :

- **Q1**: Existe-t-il une stratégie d'entreprise positionnant l'adoption des solutions cloud ?
- **Q2**: Existe-t-il un *framework* chargé de l'adoption des solutions *cloud* ?
- **Q3**: Existe-t-il des indicateurs clés de performance (KPI) afin de contrôler la performance durant l'adoption des solutions *cloud* ?
- **Q4**: La structure organisationnelle est-elle adaptée à l'implémentation des solutions *cloud* ?
- **Q5**: Existe-t-il des formations dédiées aux solutions *cloud* pour vos employés ?
- **Q6**: Quel est le rôle de la DSI durant l'adoption des solutions *cloud* ?
- **Q7**: Existe-t-il un plan de communication positionnant le *cloud* et ses impacts au sein de l'entreprise ?
- **Q8**: La gestion des risques est-elle mise à jour pendant l'adoption des solutions *cloud* ?
- **Q9**: Existe-t-il un *framework* de conformité (*compliance framework*) adapté pour l'adoption des solutions *cloud* ?
- **Q10**: Existe-t-ils des modèles de contrats *cloud* pour les fournisseurs ?
- **Q11**: Les outils de la gestion des projets sont-ils mis à jour afin de soutenir les projets *cloud* ?
- **Q12**: Existe-t-ils des compétences dans la gestion des projets *cloud* ?
- **Q13**: Existe-t-ils des processus définis pour l'architecture *cloud* ?
- **Q14**: Existe-t-ils des processus (ITIL, CoBiT) définis pour la gestion des risques et des services *cloud*, et pour la conformité ?
- **Q15**: Pour les entreprises adoptant des solutions IaaS: Existe-t-il un contrôle et une gestion totale des solutions IaaS ?
- **Q16**: Pour les entreprises adoptant des solutions PaaS : Existe-t-il un *framework* disponible pour le développement correct des solutions PaaS ?
- **Q17**: Pour les entreprises adoptant des solutions SaaS : Existe-t-il une politique d'entreprise pour l'implémentation conforme et effective des solutions SaaS ?
- **Q18**: Les compétences de sécurité sont-elles mis à jour afin d'inclure les exigences requises par l'adoption des solutions *cloud* ?

Nous avons commencé par calculer la maturité de chaque domaine, permettant aux entreprises d'améliorer ceux qui présentent une maturité non développée. Ceci nous a mené à la moyenne de maturité totale de chaque entreprise. L'analyse identifie trois groupes ayant comme maturité : CMM3 (IT.16, IT.7, IT.24 et IT.5), CMM2 (IT.8, IT.12, IT.3, B.9, IT.14, IT.11, IT.18, IT.22, B.11, IT.15, IT.2, B.6, B.10, IT.4, B.4, IT.23, IT.21, IT.13, B.8, IT.6, IT.17, IT.9, IT.10, IT.20, et B.5), ou CMM1 (IT.19, IT.1, B.1, B.2, B.7, et B.3).

## II. Analyses de groupes

Le premier groupe classifié CMM3 possède une maturité de niveau 3 sur 5, ce qui signifie que les entreprises sont sur la bonne voie d'adoption maturité en termes de leurs solutions *cloud*. En se basant sur la note attribuée à chaque question, nous pouvons conclure que les entreprises de ce groupe ont actualisé la gestion de leurs risques et leurs compétences en termes de sécurité. Les risques générés par les solutions *cloud* ne jouent pas un rôle d'inhibiteur pour ces entreprises, bien au contraire, ces dernières apprennent à les affronter et donc à les mitiger. De plus, elles offrent des formations *cloud* pour leurs employés afin de les guider dans la gestion des solutions adoptées. Ces entreprises se focalisent amplement sur l'adoption d'un *framework* de conformité, des mécanismes de gouvernance dévoués au *cloud*, une stratégie d'entreprise positionnant l'utilité du *cloud*, et enfin un *framework* d'adoption.

Bien que ces entreprises montrent une maturité plus développée que les autres, il existe néanmoins quelques points sur lesquels elles doivent encore s'améliorer. Par exemple, elles peuvent fortifier le rôle de leur DSI, augmenter la communication entre les départements, se baser sur des indicateurs de performance et développer leurs plates-formes et infrastructures *cloud*.

Le groupe 2, classifié CMM2, possède une maturité de niveau 2 sur 5. Tandis que ces entreprises sont conscientes des différents bienfaits générés par les solutions *cloud*, elles sont encore méfiantes vis à vis des risques, ce qui inhibe leur adoption. Il s'avère que ces entreprises ont développé la gestion des risques et les compétences en termes de sécurité. Alors que certaines développent les processus de leurs architectures, d'autres s'occupent seulement de leurs structures. Ceci montre qu'elles comprennent le rôle important que joue les mécanismes dans les entreprises afin de devenir plus matures. Par ailleurs, quelques-unes actualisent leurs stratégies et d'autres leurs infrastructures.

Néanmoins, les entreprises appartenant au groupe 2 doivent améliorer plusieurs points comme favoriser plus de communication entre les départements, offrir des formations dédiées aux solutions *cloud*, développer les compétences en termes de projets *cloud*, mettre à jour les outils nécessaires pour les projets *cloud*, fortifier le rôle de leurs DSI, et se focaliser sur les contrats avec leurs fournisseurs *cloud*.

Le dernier groupe 3, classifié CMM1, possède le plus bas niveau de maturité (1 sur 5). Ces entreprises sont contrôlées par les risques de sécurité et de conformité. Elles doivent développer un *framework* d'adoption, une stratégie d'entreprise prenant en compte les solutions *cloud*, des mécanismes de gouvernance dédiés à ces solutions, et également des compétences nécessaires. De plus, il leur est conseillé d'adopter des indicateurs de performance et de créer plus de communication entre les divers départements de l'entreprise.

## III. Analyse approfondie

Afin d'approfondir nos résultats, nous avons analysé les décisions prises, les décideurs responsables, les mécanismes adoptés par ces trois groupes d'entreprises, leur niveau de compétences acquises, ainsi que les motivations les poussant à adopter des solutions *cloud*.

Le groupe 1 a implémenté plusieurs mécanismes (structures, processus, relationnels). Etant donné que la gouvernance des TIC est influencée par l'implémentation des mécanismes et que le *cloud* fait partie des TIC de l'entreprise, le niveau de maturité du *cloud* dépendra du niveau de maturité des mécanismes adoptés par l'entreprise. Ceci explique donc la maturité plus élevée comparée aux deux autres groupes. Par ailleurs, les entreprises du groupe 3 partagent la même motivation (la compétition), mode de décisions (décentralisé), prise de décisions (collaboration), et un niveau de compétences développées plutôt élevé.

En revanche, le groupe 2 ne possède pas autant de mécanismes que le groupe 1, ce qui peut justifier que leurs maturités soient moins développées. D'une part, la majorité des entreprises est poussée par les bienfaits économiques générés par le *cloud*, et d'autre part, certaines sont poussées à adopter des solutions *cloud* afin d'être innovantes. Ces dernières sont décentralisées et la prise de décisions s'y fait par une collaboration entre les départements.

Même si elles désirent adopter plus de solutions sophistiquées, elles ignorent les étapes à suivre, ce qui souligne l'importance des formations et du développement des compétences utiles aux employés, et donc à la performance des entreprises. Cependant, les entreprises centralisées possèdent une maturité encore moins développée, due au contrôle total par la DSI.

Le groupe 3 représente les entreprises possédant un niveau d'intensité d'adoption des solutions *cloud* (et donc une maturité *cloud*) très bas. Ces entreprises sont toutes centralisées, majoritairement motivées par la réduction des coûts et contrôlées par la DSI. Il est important de noter que les quelques mécanismes implémentés par ce groupe ne sont même pas dédiés au *cloud*.

## IV. « Cloud Governance Framework »

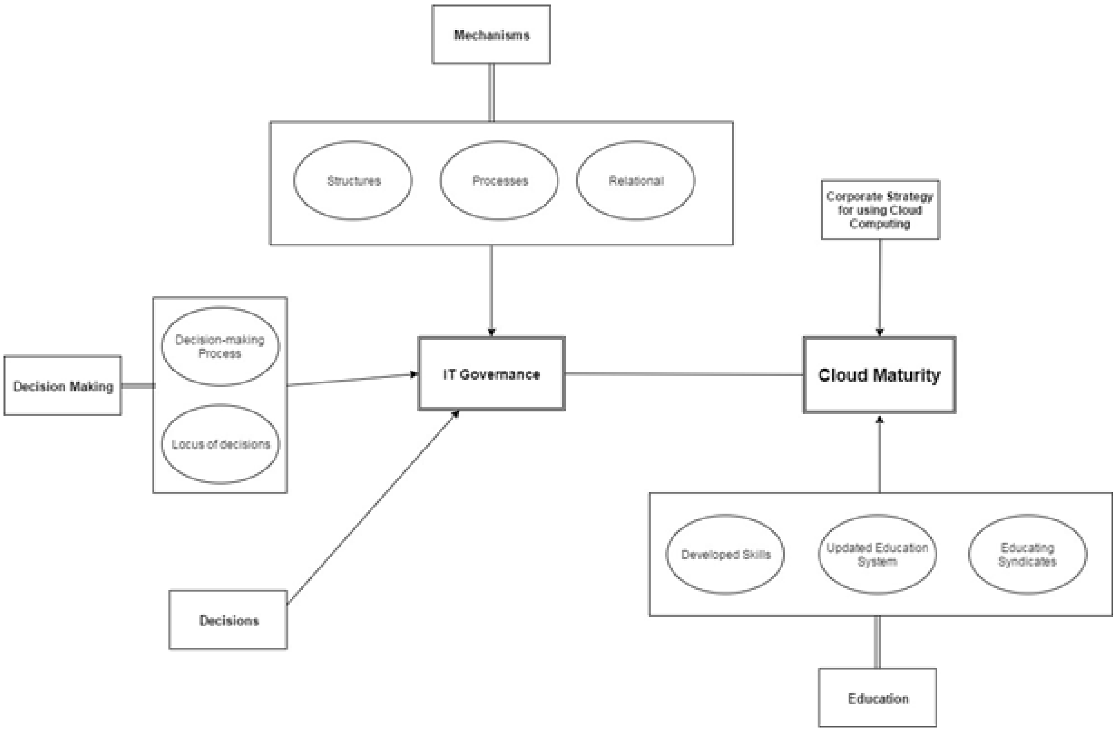


**Figure 42:** ***Cloud Governance Framework*** **(source: auteurs)**

Sur la base des premier et second tours d'entretiens, nous avons conçu le *cloud governance framework*, représenté dans la Figure 1. Ce *framework* illustre d'une part les facteurs affectants la gouvernance des TIC (*IT governance*) et d'autre part, les facteurs affectants le niveau d'intensité d'adoption des solutions *cloud* (*cloud maturity*).

En ce qui concerne la première partie, il s'est avéré que la gouvernance des TIC pour les entreprises adoptant des solutions *cloud* est influencée par les décisions adressant des problématiques liées au *cloud*, la prise des décisions liées au *cloud* où le rôle de la DSI est important ainsi que le mode de décisions, et enfin l'adoption de mécanismes de gouvernance liés au *cloud*. Tant que ces trois facteurs sont bien mis en place, les solutions *cloud* ainsi que les TIC pourront être gouvernées efficacement.

Le niveau d'intensité d'adoption des solutions *cloud* est affecté par ces facteurs : la motivation pour adopter des solutions *cloud* et le niveau d'éducation qui est également influencé par les compétences développées par les employés, le système d'éducation et l'éducation des syndicats. De surcroît, ce *framework* peut aider les entreprises à s'auto-évaluer afin d'acquérir un niveau de maturité plus élevé. Par ailleurs, le *cloud governance framework* souligne un lien de corrélation entre la gouvernance des TIC avec des solutions *cloud* adoptées au sein d'une entreprise et son niveau d'intensité d'adoption des solutions *cloud*.

## V. Modèles de gouvernance

Fondés sur la classification des trois groupes d'entreprises, nous avons pu déduire quatre modèles de gouvernance différents. Ces modèles se distinguent par le nombre de mécanismes de gouvernance dédiés au cloud adoptés par l'entreprise, le mode de gouvernance (centralisé ou décentralisé), le processus de la prise de décisions (par la DSI ou en collaboration), le nombre de décisions adressées liées aux solutions *cloud*, et le niveau de compétences en *cloud* acquis par les employés.

Afin d'illustrer un exemple des 4 modèles de gouvernance qui ont émergé, la Figure 2 représente le modèle de gouvernance des entreprises appartenant au groupe 1.


**Figure 43: Modèle de gouvernance du groupe 1 (CMM3)**

# Discussion des résultats

## I. Le cloud accompagné de la gestion du changement

L'arrivée des solutions *cloud* en entreprises a changé le rôle traditionnel de la DSI ; le seul département qui était en charge de contrôler les TIC. La DSI est désormais responsable de l'acquisition des solutions *cloud* les plus adaptées à l'entreprise. Elle est donc responsable des analyses comparatives et de la négociation des contrats *cloud*, afin d'en approvisionner de chez des fournisseurs adéquats. Dès lors, les employés de la DSI se trouvent obligés de développer des compétences en matière de *benchmarking*, négociation, contrats *cloud*, et de finance, afin de pouvoir prendre part aux décisions liées à l'acquisition des solutions *cloud*. De même, ces dernières ont modifié la relation entre les départements métiers et la DSI, où ceux-là possèdent désormais la possibilité de mettre en œuvre des solutions indépendamment de la DSI. Ceci pousse la DSI à devenir proactive plutôt que prescriptive, afin de s'orienter vers les besoins des métiers. Par ailleurs, par l'adoption des solutions *cloud*, l'entreprise passe d'une sécurité technique à une sécurité contractuelle, et de nouvelles compétences sont attendues de la part de la DSI. La notion de contrats gagne désormais de l'importance pour les entreprises adoptant des solutions *cloud*. En outre, ces entreprises transforment leur modèles traditionnels basés sur une gestion de projets rigide en modèles plus agiles ; d'où la naissance du concept des DevOps par exemple.

L'adoption des solutions *cloud* pousse les entreprises à gérer leurs salariés différemment, surtout en présence du télétravail. Les managers sont alors confrontés à de nouveaux challenges afin de contrôler le travail et la présence de leurs salariés au bureau. Avec l'arrivée des solutions cloud, les entreprises sont invitées à modifier leurs politiques et les managers sont ainsi encouragés à changer leurs leaderships.

Cependant, par suite de tous les changements engendrés par les solutions *cloud*, l'adoption doit être perçue comme un projet de gestion du changement impliquant plusieurs parties prenantes. C'est pourquoi afin de faciliter leurs transitions vers le *cloud*, les entreprises déploient la conduite du changement (*change management*).

De surcroît, à l'aide d'une analyse des parties prenantes (*stakeholder analysis*) les entreprises sont capables d'identifier les différentes parties prenantes essentielles au processus d'adoption des solutions *cloud*, pour ensuite analyser leurs contributions dans les projets de la gestion du changement (Moir, 2001). En effet, grâce à nos analyses, nous avons pu identifier une partie prenante indispensable mais non mentionnée par la littérature : les syndicats. Le rôle des syndicats est de représenter la voix des salariés afin de protéger leurs travails. Selon nos participants, les syndicats perçoivent le *cloud* comme menace aux salariés de la DSI, et donc s'y opposent fortement. Il est donc important de former ces syndicats afin qu'ils soient d'accord avec les décisions des entreprises.

Au-delà de l'analyse des parties prenantes, les entreprises doivent définir et intégrer des formations éducatives, soutenues par le département des ressources humaines. Ce dernier doit intégrer ces formations à ses politiques afin de soutenir le changement qui a lieu au sein de l'entreprise.

Par conséquent, la gestion du changement constitue une étape primordiale afin d'adresser les transformations liées aux solutions *cloud*.

## II. L'adoption des solutions *cloud* et la gestion des risques

La gestion des risques est essentielle pour les entreprises adoptant des solutions *cloud* étant donné que ces dernières engendrent de multiples risques (fuites et perte de données, interopérabilité, conformité, attaques externes, etc.) Comme mentionné antérieurement, le développement des compétences de traitement des contrats *cloud* est nécessaire afin de minimiser les risques possibles. Tous ces risques ont émergé à cause de nombreux exemples de violations de la sécurité qui ont atteint la sensibilité des données des entreprises. Par conséquent, les fournisseurs doivent rassurer leurs clients de la confidentialité et la sécurité des solutions qu'ils offrent afin de respecter leur « *data privacy* ». Ceci donne naissance à une nouvelle relation entre les entreprises et leurs fournisseurs *cloud*, où ces derniers font partie de l'écosystème du marché *cloud*. Cette relation doit être pourtant basée sur la confiance, le respect et la réciprocité.

Par ailleurs, la présence d'un autre risque s'amplifie au sein des entreprises et accompagne l'émergence des solutions *cloud* : le « *shadow IT* ». L'analyse de nos résultats montre que les perceptions de nos participants par rapport au « *shadow IT* » sont divergentes. Alors que certains le perçoivent en tant que risque, d'autres le considèrent comme activité normale au sein de l'entreprise. Ceci accentue le besoin d'une analyse des parties prenantes afin d'identifier différentes façons d'aider les entreprises à faire converger les perceptions et objectifs de leurs parties prenantes.

Alors que l'alignement des solutions *cloud* avec la stratégie de l'entreprise et son infrastructure l'aide à bénéficier des avantages promis, l'adoption de telles solutions demeure exigeante. D'ailleurs, les managers anticipent que durant le processus de prise de décisions, la distribution de pouvoir devra être redéfinie afin que les directions métiers puissent y participer.

Par conséquent, avec toutes ces transformations affectant les entreprises ainsi que le transfert du pouvoir de la DSI aux directions métiers, les solutions cloud ne sont toujours pas adoptées de façon optimale, ce qui accentue le besoin de les gouverner effectivement.

## III. Gouvernance des solutions *cloud*

Etant donné que dans la littérature, aucun modèle de gouvernance ne se penche sur tous les aspects primordiaux des solutions *cloud*, ce qui nous a poussé à explorer si ces dernières nécessitent une gouvernance des TIC spécifiques, en se basant sur 35 grandes entreprises françaises. Nous nous sommes appuyés sur la définition de la gouvernance des TIC proposée par Luftman et Brier (1999), Sambamurthy et Zmud (2000), Peterson (2004), et Weill (2004). Ces derniers suggèrent, tout d'abord, d'explorer les décisions liées aux TIC (celles du *cloud* pour notre cas). En revanche, la littérature ne semble pas s'intéresser aux décisions nécessaires pour l'adoption des solutions *cloud*. Par conséquent, en se basant sur les réponses reçues par nos participants, plusieurs décisions ont été notées. Ceci pousse les décideurs à les rajouter aux décisions liées aux TIC en tant que première étape de gouvernance. Par la suite, la gouvernance des solutions *cloud* nécessite une attribution de pouvoir de ces décisions aux parties prenantes les plus adéquates. Derrière la façade simple de ce processus se cache des couches plus complexes que plusieurs auteurs ont traité selon différents axes (droits de contrôler des décisions, et droits de gérer des décisions). Nous avons, toutefois, exploré ce processus comme un seul axe globale et intégrale, ce qui représente une limite à notre travail de recherche. Il serait intéressant d'ajouter que la DSI est responsable de la prise de décisions dans toutes les entreprises centralisées interviewées, ce qui confirme l'hypothèse de Tiwana (2009) (de même pour les entreprises décentralisées où le processus se déroule suivant une collaboration des départements). En sus de l'attribution des décideurs, les entreprises s'occupent d'implémenter des mécanismes de gouvernance mêlant structures, processus, et mécanismes relationnels. Ils visent à coopérer afin de guider les départements et les encourager à opter pour un comportement organisationnel spécifique (Weill et Ross 2004; De Haes et Van Grembergen 2009; Simonsson et al., 2010). Par ailleurs, lorsque ces mécanismes sont implémentés ensembles, ils forment le système de gouvernance des entreprises. La littérature ne s'intéresse cependant pas assez aux mécanismes nécessaires lors de l'adoption des solutions *cloud*.

A l'issue de la nécessité de différentes prises de décisions liées aux solutions *cloud*, décideurs, et mécanismes de gouvernance, nous pouvons répondre à notre question de recherche en affirmant que le déploiement des solutions *cloud* requiert, en effet, une gouvernance des TIC spécifique.

## IV. Modèles de gouvernance *cloud*

Après avoir déduis que les solutions *cloud* nécessitent des modèles de gouvernance des TIC spécifiques, nous avons décidé d'explorer le niveau d'intensité d'adoption des solutions *cloud* de ces entreprises (i.e. leurs niveaux de maturité). Ceci nous permettra d'étudier les différents facteurs affectant leur maturité ainsi que leur gouvernance. En se basant sur les facteurs révélés, quatre modèles de gouvernance différents ont émergé. Ces modèles soulignent la nécessité d'une gouvernance spécifique lors de l'adoption des solutions *cloud*.

## V. Limites de notre travail

Plusieurs facteurs ressortent de nos analyses : décisions, décideurs, mécanismes de gouvernance, éducation des salariés, et motivation de l'entreprise. Pourtant, ces facteurs possèdent la même pondération ; i.e. tous les facteurs contribuent à la gouvernance de l'entreprise de la même manière. Dès lors, notre travail de recherche semble limité étant donné que certains facteurs peuvent avoir une influence plus remarquable que d'autres.

Par ailleurs, à l'aide de nos analyses, nous avons été capables de confirmer la présence d'un lien de corrélation entre la gouvernance des entreprises adoptant des solutions *cloud* et leurs niveaux d'intensité d'adoption. Nous n'avons cependant pas eu la possibilité d'explorer la présence d'un lien de causalité entre ces derniers. Ceci forme une autre limite à notre travail de recherche.

De surcroit, l'analyse de nos résultats adresse la présence de « *shadow IT* » en entreprises sous différentes formes. Nous avons exploré les raisons menant aux activités de « *shadow IT* » au sein des 35 entreprises, les modèles de services utilisés, et l'impact de ces activités. En revanche, il serait aussi intéressant d'explorer le lien de corrélation (possible) entre les activités de « *shadow IT* » et le niveau d'intensité d'adoption des solutions *cloud* des entreprises.

Il faut aussi noter que le système d'éducation ainsi que la formation des syndicats ressortent comme facteurs impactant l'adoption des solutions *cloud*. Pourtant, aucune littérature n'existe afin de soutenir nos résultats. Comme le système d'éducation est lié aux formations des étudiants, il serait important de les former dès leurs parcours académiques avant leurs arrivées au monde professionnel. De même, les syndicats doivent être formés afin de soutenir les entreprises dans leurs transitions.

## VI. Pistes de recherches futures

Compte tenu des limitations citées antérieurement, plusieurs opportunités s'ouvrent afin de compléter notre travail de recherche.

Premièrement, nous pouvons tester notre modèle théorique (*cloud governance framework*) au sein de différentes entreprises internationales. Ceci nous permettra à valider notre modèle après l'avoir testé et amélioré.

De surcroit, une étude longitudinal pourrait être intéressante afin d'explorer le lien de causalité entre la gouvernance et le niveau d'intensité d'adoption des solutions *cloud*. Ceci permettra aux entreprises d'élaborer la relation de « cause à effet » entre ces derniers.

De même, une étude comparative, qui posterait sur les entreprises adoptant des méthodologies agiles et traditionnelles, pourra explorer l'effet des solutions *cloud* sur les entreprises agiles. En effet, mener des entretiens avec des parties prenantes associées aux deux environnements (agile vs traditionnel) nous aidera à identifier des « *best practices* » dont les entreprises ont besoin durant l'adoption des solutions *cloud*.

Par ailleurs, une étude approfondie pourra être menée afin d'explorer une corrélation possible entre le niveau d'intensité d'adoption des solutions *cloud* et les activités de « *shadow IT* ». La présence d'une corrélation pourra enfin révéler une solution aux activités de « *shadow IT* ».

Enfin, analyser la pondération de chaque facteur de notre *framework* constitue une étape importante ainsi qu'une valeur ajoutée à la littérature. Cette pondération mettra en valeur les facteurs ayant un impact plus élevé sur la gouvernance et l'adoption des solutions *cloud* de l'entreprise. Cela guidera les entreprises a identifié les facteurs qui permettront d'améliorer leurs gouvernance et ainsi favoriser leurs adoptions.

## VII. Contributions

### 1. Apports théoriques

Notre analyse des résultats souligne plusieurs facteurs influençant l'entreprise lors de l'adoption des solutions *cloud*. Notre travail de recherche ainsi apporte de nouvelles contributions à la littérature, telles que les transformations affectant le rôle de la DSI, l'acquisition du pouvoir par les directions métiers, et l'émergence d'une co-construction entre les différents départements. Même si le besoin de développer des compétences existe dans la littérature, nos résultats accentuent son influence sur l'adoption des solutions *cloud*. De surcroit, des éléments importants, pourtant non cités par la littérature, émergent : mettre à jour le système d'éducation français ainsi que former les syndicats à l'importance des nouvelles technologies. Nous présentons aussi des contributions surtout par un nouveau modèle de gouvernance pour les solutions *cloud* qui soulignent de nécessaires décisions, décideurs, structures, processus et mécanismes relationnels.

Enfin, à l'aide de notre *framework*, nous avons pu prouver la présence d'une corrélation entre la gouvernance des solutions *cloud* et le niveau d'intensité d'adoption. Cette corrélation s'avère importante pour les entreprises voulant se lancer dans le monde du *cloud computing*.

### 2. Apports managériales

Les entreprises ayant pour objectif la transition vers le *cloud*, doivent prendre conscience des multiples transformations à gérer, et adresser les différents impacts générés par le *cloud*. Selon les décisions mentionnées par nos participants, les entreprises peuvent ainsi étudier leur transition par le biais de multiples collaborations et discussions entre les départements. Ceci améliora leurs gouvernances et favorisera leur adoption. En effet, les entreprises pourront investir dans les formations pour leurs employés (sur des plateformes internes ou externes). De surcroit, à l'aide d'une gouvernance effective, les entreprises peuvent lutter contre les risques engendrés par les solutions *cloud*. Enfin, les entreprises peuvent se baser sur les modèles de gouvernance proposés afin d'améliorer leur gouvernance et leur adoption.

# Conclusion

Depuis l'émergence des TIC et leur évolution, les entreprises sont davantage sensibilisées aux apports générés par ces technologies. C'est le cas notamment de l'amélioration de la performance de l'entreprise, la création de valeur au sein même de celle-ci, l'alignement de la stratégie de la DSI et des directions métiers, et la gestion des risques liés au SI. Les solutions *cloud* font partie de l'évolution des TIC. Cependant, les travaux de recherche réalisés soulignent l'existence de risques engendrés par ces solutions. Par ailleurs, elles transforment les grandes entreprises sous différents axes ; la transition du pouvoir des mains de la DSI à celles des directions métiers, la nécessité de développer des compétences afin de savoir manipuler des solutions *cloud* – surtout des compétences pour pouvoir méticuleusement lire et comprendre les contrats avec les fournisseurs, l'émergence d'activités de « *shadow IT* », ainsi que des transformations des processus, infrastructure, et méthodologies. Pourtant, grâce à une gouvernance effective des solutions *cloud*, l'entreprise pourra bénéficier de ces nombreux avantages tout en réduisant les risques générés.

A ce jour, les modèles de gouvernance matures du *cloud* sont peu ou prou présents dans la littérature. Ceci a encouragé ce travail de recherche à s'intéresser à la gouvernance de ces solutions afin de proposer un modèle théorique. En se basant sur la définition de la gouvernance des TIC proposée par Luftman et Brier (1999), Sambamurthy et Zmud (2000), Peterson (2004), et Weill (2004), nous avons décidé d'explorer la possibilité de gouverner les solutions *cloud* par le biais de la gouvernance des TIC de l'entreprise. Ainsi nous avons mené deux phases d'entretiens avec une trentaine d'employés de la DSI et des directions métiers. Les résultats tirés de la première phase d'entretiens ont révélé d'une part les transformations menées par l'adoption des solutions *cloud*, d'autre part la présence du « *shadow IT* », et finalement la nécessité d'une gouvernance spécifique pour les solutions *cloud*.

Cette première phase a mis en évidence la possibilité d'un rapport entre gouvernance effective des solutions et le niveau de maturité de ces solutions. Ceci a conduit à un second tour d'entretiens avec les mêmes entreprises afin d'étudier le niveau d'intensité de leurs adoptions (leurs maturités). Les résultats du second tour d'entretiens montrent que dans le but de posséder un niveau de maturité élevé en solutions cloud, les entreprises doivent prendre des décisions liées au *cloud* et avoir une gouvernance décentralisée, une DSI à l'écoute des métiers, plusieurs mécanismes spécifiques au *cloud*, des compétences et connaissance en *cloud* plutôt avancées, une vision ouverte et novatrice accueillant les nouvelles technologies et le changement qui en découle, et enfin être motivés par la compétition (illustré par le premier modèle de gouvernance émergeant). En se basant sur la première et deuxième partie d'analyses, nous avons conçu un « *cloud governance framework* » qui montre les différents facteurs affectant la gouvernance spécifique des solutions *cloud* et ceux affectant le niveau d'intensité d'adoption des solutions *cloud*.

Par ailleurs, l'adoption des solutions *cloud* est influencée par les différentes perceptions et interactions des parties-prenantes, qui eux-mêmes sont influencé par cette adoption. Il s'avère, donc, important de conduire une analyse des parties-prenantes (« *stakeholders analysis* ») ainsi qu'une approche de conduite du changement (« *change management* »). Ces analyses sont nécessaires afin de faciliter la prise de décisions parmi les différentes parties-prenantes (avec l'émergence des fournisseurs en tant que nouvelles parties-prenantes) et faciliter la transition vers un environnement *cloud*.

*French Summary*

Notre travail de recherche aborde la gouvernance des TIC, sur laquelle les entreprises peuvent se baser afin de concevoir une gouvernance spécifique aux solutions *cloud*, ce qui répond à notre question de recherche. Aujourd'hui, rares sont les écrits à avoir mobilisé un modèle pour gouverner les solutions *cloud* de manière effective. De même, le lien entre cette gouvernance et le niveau de maturité de ces solutions n'a pas été exploré. Ce travail contribue ainsi à la littérature de la gestion des Systèmes d'Information, spécifiquement à celle du *cloud*. En se basant sur les travaux de recherche antérieurs, nous avons pu tout d'abord identifier les éléments nécessaires afin de gouverner les solutions *cloud*. De plus, en se basant sur le modèle de maturité proposé par l'Open Data Alliance Center®, nous avons pu classifier les entreprises selon leurs différents niveaux de maturité. Ce travail contribue donc également à la littérature des modèles de maturité. Enfin, notre « *cloud governance framework* » permet aux entreprises d'évaluer leur maturité et d'identifier le(s) domaine(s) qui nécessite(nt) des améliorations.