Keiwan Babani
IT Risk and Assurance
December 2016

The sky is the limit

A migration to cloud and its impact on the IT audit

Building a better
working world

The sky is the limit

A migration to cloud and its impact on the IT audit

Master Thesis
School of Economics and Management
Tilburg University
December 2016
EY, Eindhoven

1st supervisor : Dr. J. Hulstijn

2nd supervisor : Dr. M. Smits

Company supervisor EY : Erik Smeets

Company guide EY: Dominique Kuijs

Name : Keiwan Babani

ANR : 938684

Topics : Cloud computing/Auditing/Risk Assurance/ Data integrity

Study Program : Master of Information Management (MSc IM)

Academic Year : 2016-2017

Number of words : 22,774

Management Summary

Cloud computing is an evolving paradigm, that is being implemented among organizations. Although cloud computing as a technology, has become very attractive to organizations, it seems that companies are underestimating its effects and risks, whenever they decide to migrate their applications and data to a shared cloud environment with numerous users.

Cloud computing and its underlying security risks can affect organizations that have either outsourced parts or all of their data or applications to a cloud environment. These security risks have a potential influence on the performed IT audit activities. IT audits are performed to examine whether an organization's information systems and included operations and management follow a set of guidelines and standards, in order to ensure reliability of reporting, business continuity and compliance on behalf of stakeholders such as the general public. It is of interest to investigate the effects of a migration to cloud on the data integrity of an organization and its subsequent effect on the IT audit.

Here lies the main interest of this research, inspecting the migration of an organization to cloud computing, what this means for data integrity, what risks impact the data integrity and how this in turn affects the IT audit. The central question to study these effects is defined as follows:

> What is the impact of an organization's migration to a cloud environment and how does it influence the IT audit method?

Based on a case study involving two healthcare organizations and four IT auditors of different management levels, evidence was found that organizations do not make the proper considerations before migrating to cloud, even underestimating the possible risks and effects it can have. Quite possibly, data integrity can be affected on the cloud and it remains uncertain whether data integrity is being maintained all the time. Caused by the migration to cloud, IT auditors have less work related to the specific client applications being audited and are less present at the clients. Moreover, their IT audit activities have gradually changed from actual testing to the review of assurance statements. This has thereon affected the relationship between the IT auditor and the client to a certain degree.

Preface

This master thesis concludes my master Information Management at Tilburg University. Commissioned by EY, I have completed this last phase of my study performing a research for six months on the impact of an organization's migration to cloud and its subsequent effects on the IT audit.

Hereby, I would like to thank some people who have supported me during my research. First of all, I would like to thank my university supervisor Dr. Joris Hulstijn. I admire the knowledge he has demonstrated and the insights he provided related to my research topic. He was always ready to provide me with the necessary feedback, provided clear comments and was quick in his replies to my emails, which I have very much appreciated.

I would like to thank my company guide Dominique Kuijs for always being available and ready to guide me through my master thesis, providing me with very insightful and critical feedback. I enjoyed his advice and to me it felt like he was a friend rather than a company guide, and as such I regard him.

I would like to thank my company supervisor Erik Smeets for making me feel very comfortable at EY, guiding me and providing me with the necessary advice. I very much appreciate his guidance, helping me find this master thesis's topic and case organizations for my research.

Finally, I would like to thank my colleagues at EY, who through the last six months have been available for discussions, thinking along and providing me with feedback.

Keiwan Babani
Eindhoven, December 2016

Table of contents

1. Introduction

This chapter introduces the research topic, problem indication as well as the research questions. Subsequently, the scope is defined and research progress is expanded upon. Additionally, the goal of the study as well as the theoretical and practical relevance are discussed.

1.1 Problem indication

Cloud computing is an evolving paradigm, that is being implemented among organizations. While cloud computing as a technology, has become very attractive to organizations, its effects and risks are still being underestimated. Cloud computing operations can be seen as the practice of information systems outsourcing. The similarity between the two lies in the use of an external vendor’s hardware, software, infrastructure or storage proficiencies for internal ICT processes. Organizations migrate to cloud computing practices in order to increase their efficiency, flexibility, agility and their scalability potential, while saving costs (Chou, 2015). While cloud computing is gaining popularity due to the benefits it brings, it still remains a work in progress. The services provided by cloud service providers not only enforce traditional security risks to a certain degree due to its ubiquity, but it also introduces additional security threats (i.e. shared technology issues and cloud abuse). The migration of an entity’s assets (data, applications, etc.) to a shared cloud environment with numerous users sharing and using cloud resources and having the assets outside of the administrative control, escalate security concerns (Ali, Khan, & Vasilakos, 2015). These security issues range from trust issues and reliability to data security and integrity concerns, which also affect the organizations and the IT audits being performed. IT audits are a process of examination of the management and internal controls within an IT infrastructure. Hence, the importance that these security issues and data integrity concerns are properly mitigated.

Growth in 2014 accelerated for the Big Four accounting firms: Deloitte & Touche, Ernst & Young (EY), KPMG and PricewaterhouseCoopers (PwC) to a record $120 Billion, with the audit revenues of the firms amounting to $50 Billion US dollars (Big4, 2015). Undoubtedly, the revenues of the entire auditing industry is even greater. Part of the activities of the Big Four accounting firms is performing IT audits. IT auditing however, is very broad since public organizations have adopted IT for processing all of their business data, meaning that no matter the adopted business model, all data and messages would be handled by ICT systems. For this reason, the Big Four and accounting firms in general are constantly researching new IT trends and their impacts to expand their knowledge and increase the effectiveness of their audits.

The main purpose of IT auditing is to examine whether an organization's information systems and included operations and management follow a set of guidelines and standards, in order to ensure reliability of reporting, business continuity and compliance on behalf of stakeholders such as the general public. Recently, more and more companies have adopted cloud computing services and with this rise, cloud computing has attracted IT auditors' attention, regarding the possible risks associated with such technologies since it crucially affects their work. With these circumstances, IT auditors must understand the details regarding cloud computing. Cloud computing brings changes to organizations and these changes affect the performed audits, possibly resulting in an adjustment in IT audit activities and tools. With the involvement of outside vendor's support and control and cloud computing being prone to many security and integrity risks, the auditing work can be more complicated than the regular IT auditing work (Chou, 2015). Or conversely, it could be less complicated because processes are more standardized in the cloud. That is for this research to find out.

Former studies have outlined possible effects of cloud computing security risks in general on organizations (Ali, Khan, & Vasilakos, 2015; Cloud Security Alliance, 2011; Ramgovind, Eloff, & Smith, 2010). It is in the IT auditor's interest to have a clear idea of the effects of an organization's migration to a cloud environment and how this affects the way they conduct their IT audit.

This research focusses on data integrity, which refers to the consistency and accuracy of data over its entire life-cycle. Clients need to have the right controls in place that mitigate risks and prevent misstatements that could affect the data integrity. IT audits are performed to test controls and mitigate information risks, in order to provide assurance to the clients that the financial statements are reported accurately and free of misstatements. To further investigate data integrity and how it is affected, the Clark and Wilson model is used. The Clark and Wilson model is an integrity policy model with the goal of ensuring integrity of data to prevent fraud and errors. This research studies in what way the Clark and Wilson model and its key aspects are affected by a migration to cloud.

1.2 Problem statement

Cloud computing and its underlying security risks can affect organizations that have either outsourced parts or all of their data or applications to a cloud environment. Subsequently, these security risks can have a potential influence on the scheduled and performed IT audit activities. According to Chou (2015) security risks are the most significant concern to cloud computing, meaning migrations to a cloud environment or being on the cloud affect the vulnerability of organizations in different ways as to traditional structures. Additionally, increasing the feeling of lack of control amongst organizations. Data integrity risks have an influence on an organization's data on the cloud. In order to increase an IT auditor's insight regarding the effects of cloud computing on the auditor's activities, it is crucial that the impact of an organization's migration to cloud is clearly outlined. To be more precisely, the effects of a migration to cloud on the data integrity of an organization and its subsequent effects on the IT audit method.

Here lies the main interest of this research, inspecting the migration of an organization to cloud computing, what this means for data integrity, what risks impact the data integrity and how this in turn affects the IT audit. The goal of this research is to examine to which extent a migration to cloud computing has an impact on the IT audit with a focus on data integrity risks. This will allow this research to outline the attention points and make recommendations based on the effects to be found.

1.3 Research questions

In order to achieve the goal of this research and provide an answer to the central problem statement investigating the effect of an organization's migration to cloud on the IT audit, a main research question and several sub-questions have been formulated. Every question looks at a different part of the study, and taken as a whole the questions, lead to the answer to the main research question. From the problem statement and the research objective the following research question has been formulated:

> What is the impact of an organization's migration to a cloud environment and how does it influence the IT audit method?

To offer an inclusive answer to the central problem statement and the main research question, three sub-questions have been formulated. The first two sub-questions provide a theoretical background on the subjects, namely:

1. What is cloud computing and what risks are involved?
2. What is the current IT audit methodology and how is it conducted?

As a follow up on the theoretical background, the third question will delve into the practical side:

3. What is the effect of an organization's migration to cloud on the data integrity risks and how does it influence the IT audit method?

A conceptual model has been made to give a clear graphical representation of the theoretical framework and the relationships between the variables, as can be seen in figure 1.

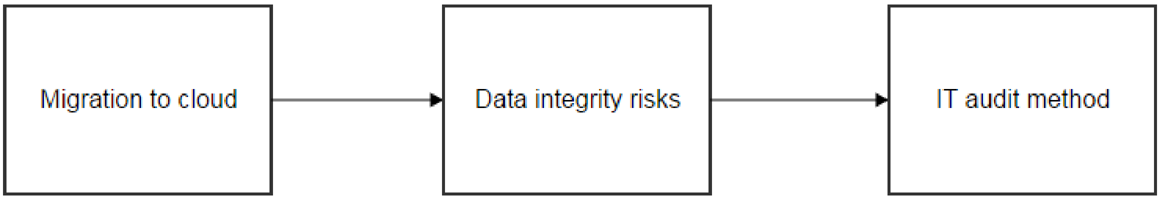

Figure 1: Conceptual model of the theoretical framework

1.4 Research method

As can be seen from the conceptual model in figure 1, this research will study the effect of an organization's migration to cloud on the IT audit. To study this relationship focus is on the data integrity risks that are affected by a cloud computing migration. The migration to cloud computing has an impact on the data integrity risks and this subsequently influences the IT audit. This research will study how organizations are affected by data integrity risks after they have migrated to a cloud environment and how this subsequently affects the IT audit.

This research adopts the action research methodology. Action research is a cyclical process that is used for studying change in organizations. During this cyclical process action and critical reflection occur in turn. Baskerville and Pries-Heje (1999) define action research as a cyclical process involving “the formulation of a theory, intervention and action-taking in order to introduce change into the study subject, and analysis of the ensuing change behavior of the study subject” (p. 1). Being a cyclical process it allows one to explore, test and assess new ideas and their effectiveness. Critical reflection is crucial at every step increasing the understanding which can be put to good use in later steps in general as knowledge or lessons learned. Action research is very responsive, making it a useful research tool for investigative research and diagnosis or evaluation.

The research consists of a theoretical and an empirical part. Starting from ‘planning’, the theoretical part of this research is used as an exploratory method to delve into the characteristics of cloud computing and IT audit with the concerned integrity risks. The exploratory method consists of a literature review in order to define the subjects and to have an explanation from theory. The literature review depends on existing relevant literature, found through available sources such as Tilburg University, complemented by Google Scholar, which allows researchers to find relevant work across the world of scholarly research.

The theoretical part provides this research with a solid background on cloud computing and the IT audit. From the literature two expectations will be formulated, about the impact of a cloud migration and its subsequent effects on the IT audit method. An important part of the action research is diagnosis or analysis, namely of the current situation and how this is affected. The formulated expectations will serve as ‘instruments’ for the analysis part of the action research cycle.

The next part of the research is empirical. The next step in this research would be to use the collected results from the literature review in a case study taking two healthcare organizations as objects of research. According to Yin (2013), a case study research would be the preferred method, whenever a researcher has little control over behavioral events and when context and phenomenon are intertwined. Which holds true for the two chosen cases. The two cases have been identified and interview candidates have been considered. The cases will be described in detail in chapter four.

The two chosen cases are comparative healthcare organizations of which one outsourcing their applications and data to an outside cloud environment, while the other is internally hosting their data and applications. In order to have a valid analysis, the two cases will be compared and cross analyzed. For the analysis part an 'instrument' is needed. In this research, the formulated expectations serve as 'instruments'.

The next step focuses on the practical alignment of the founded information. This step is the 'acting' step of the cycle and data and evidence will be collected from the cases further clarifying the evidence pertaining to the research question (Stewart & Cash, 2005). The research method will be qualitative and data will be collected through unstructured and structured interviews with IT auditors within EY. The interviews are held with different IT auditors of different management levels within EY in order to have a representative sample of IT auditors concerned with cloud computing, data integrity and the cases. During the 'observing' step the collected data will be cross analyzed and evaluations will be made with regards to the formulated expectations. Lastly, conclusions will be made at the 'reflecting' step of the cycle.

The research progress is graphically represented in figure 2. The combination of a theoretical literature review and an empirical case study provides the optimum capability to answer the main research question.

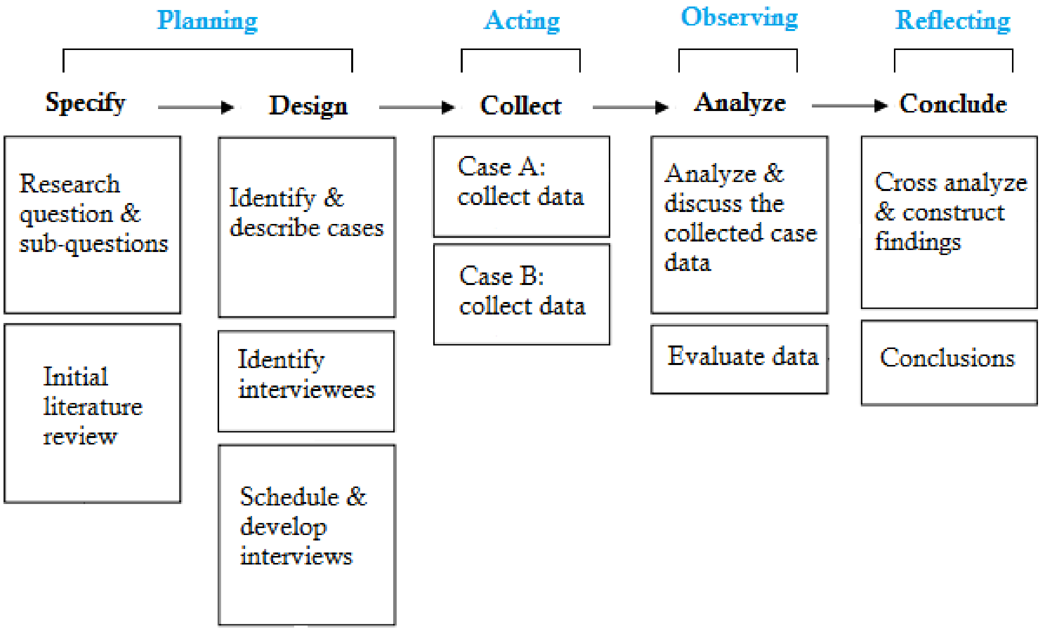
Planning
Acting
Observing
Reflecting
Specify
Design
Collect
Analyze
Conclude
Research question & sub-questions
Initial literature review
Identify & describe cases
Identify interviewees
Schedule & develop interviews
Case A: collect data
Case B: collect data
Analyze & discuss the collected case data
Evaluate data
Cross analyze & construct findings
Conclusions

Figure 2: Research progress based on the Research Protocol Flowchart *(Harvard University, 2013, p. 23)*

1.5 Scope and limitations

The research will take place under guidance of Ernst & Young (trading as EY) in Eindhoven, Netherlands. The setting at EY provides the advantage of the ability to rely on the practical knowledge that the firm has collected by years of experience. The research is performed within the IT Risk and Assurance (ITRA) or often called Financial Audit and IT (FAIT) department at EY. During this period, a literature review has been performed in order to study the relevant literature and structured and unstructured interviews will be performed with IT auditors at EY during and outside of the conducted cases.

The case study will be limited to two selected healthcare organizations of which one that outsources their data to an outside cloud environment and one using a traditional non-cloud structure (internally hosted). The two selected case organizations Motion Health and Center Clinic will be existing clients of EY. One of the cases is limited to the public cloud deployment model with the SaaS service model. Other cloud models are not being considered. Furthermore for both cases, the research is limited to only certain applications more specifically the cloud hosted application ONS from Nedap, and the internally hosted application EPIC. Both applications are similar in scope and size. The goal of this research is not to discover new techniques or create any roadmaps. The purpose of this research is to analyze the findings from the cases and to describe the effects of a client’s migration to a cloud environment. To outline what the effects are on the data integrity risks and how the IT audit subsequently is affected.

1.6 Thesis structure

This report starts chapter two with a literature review of cloud computing with a theoretical background of the phenomenon including underlying risks involving data integrity. In this chapter existing literature is explored on the subject and a theoretical background is built for subsequent chapters. Additionally, chapter two will highlight the benefits and drawbacks of using a cloud environment. Chapter three elaborates on the IT audit methodology, what it means and explains the auditing activities as performed by EY. In the fourth chapter the methodology of this research will be highlighted, the case study approach is explained and a case description is given with a presentation of the interviewees. Afterwards in chapter five, the collected results from the cases will be analyzed and discussed. This research will wrap up with chapter six and elaborate on the previous chapters, coming to a conclusion. Subsequently, the limitations of the performed study will be discussed and recommendations will be made.

2. A look at cloud computing

In an era of austerity and global financial crises, cloud computing, which usually has fewer overheads and requires less capital expenditure, is a notably attractive proposition for businesses. Recent statistics and forecasts performed by Statista (2016) show that spending on public cloud infrastructure[1] is forecast to reach $38B in 2016 and is projected to reach $127B in 2026 (Statista, 2016). Cloud computing in its form is a pay-as-you-go IT technology, ubiquitous online environment and on demand. The business world is progressively adapting and moving to cloud computing solutions. A recent market analysis performed by Cisco Global Cloud Index shows that within the next three years, more than four-fifths of all data center traffic, namely 86 percent, will be based in the cloud (Cisco Global Cloud Index, 2015) .

Cloud computing is becoming an important technology to modern businesses. However, moving to a cloud environment is not a simple choice to make. The first paragraph of this chapter explores the definition and different characteristics of cloud computing. Paragraph two follows with the advantages and constraints of cloud computing. Finally, paragraph three will delve into the risks involved with cloud computing.

2.1 The cloud

Popularity and interest in cloud computing have made a burst in recent years, mostly due to advantages of having greater flexibility and the availability in obtaining more powerful and faster computing resources at a lower cost. Due to the popularity cloud computing is coined all over the web and this has led to different definitions. As a matter of fact, it seems that there is no common definition for cloud computing (Grossman, 2009). Armbrust et al. (2010) defined cloud computing as "both the application delivered as services over the internet and the hardware and systems software in data centers that provide those services" (p. 50). However, cloud computing can also be seen as a computing platform that is able to dynamically provide servers that can be configured and reconfigured to address a wide range of needs (Jaeger, Lin, & Grimes, 2008). The aforementioned characteristics are confirmed

[1] A cloud infrastructure is the collection of hardware and software that facilitates the characteristics of cloud computing containing both an abstraction layer (software deployed manifesting the cloud characteristics) and a physical layer (hardware resources to support cloud services).

and expanded on by the National Institute of Standards and Technology (NIST) giving a clear and more detailed description of cloud computing, namely: “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Mell & Grance, 2011).

Cloud computing is not a recent development. On the contrary it is the result of the development and adoption of existing technologies and paradigms; e.g. mainframe computing, virtualization (Buyya, Yeo, Venugopal, Broberg, & Brandic, 2009). The whole idea of the concept of cloud computing came to be in order to allow businesses to benefit from all these technologies without needing the expertise and know-how of each of the technologies separately. The attractiveness of cloud computing lies in its aim of enabling businesses to put more focus on core business operations instead of being impeded by obstacles in IT technologies. From the definition of cloud computing as defined by NIST, the cloud computing model is identified as a composition of five crucial characteristics namely: on-demand capabilities, broad network access, resource pooling, rapid elasticity and measured service; four deployment models: public, private, community and hybrid cloud; and three service models: SaaS, PaaS and IaaS (Mell & Grance, 2011). The characteristics, deployment models and service models will be detailed further in section 2.1.2, section 2.1.3 and respectively section 2.1.4.

2.1.1 Cloud sourcing

Whenever organizations seek to shave costs off non-core processes, when the processes need automation or when firms want to add extra capability not immediately available in their organizations, they turn to third party providers for outsourcing. Cloud computing is a form of outsourcing. Babcock (2010) goes as far as declaring cloud computing as an evolution of outsourcing. Outsourcing in its new form[2], often called cloud sourcing.

According to Lacity, Khan and Willcocks (2009) the reason organizations outsource their processes and operations is to have increased cost reduction, access to experts, flexibility and

[2] Note: not all outsourcing is cloud.

to put more focus on the organization's core competences. This also relates to cloud sourcing and why cloud computing is increasing in popularity. Cloud computing has made it increasingly easier and faster for organizations to sign on new services. Previously, organizations had to seek potential suppliers through the word of mouth, directories and endless phone calls. However, with cloud sourcing and the increasing accessibility of cloud services, organizations should not become less careful. Cloud computing has its own downsides and related security risks, which will be discussed further in section 2.2 and 2.3.

In the case of cloud sourcing, the client cedes control over its applications and data to the cloud provider. Just like regular outsourcing, cloud sourcing raises concerns about the security of the data and applications that are outsourced to the cloud provider (Julisch & Hall, 2010). Since, in the case of cloud sourcing a client's data and applications are outsourced to a shared IT infrastructure, it becomes harder for the client to use the same level of security controls. Additionally, the assignment of responsibilities has become more complex in cloud computing. This is caused by the many possible forms of deployment and service models and the extent of controls to be configured and put in place (Julisch & Hall, 2010). Clear agreements need to be made between the client and cloud provider with regards to responsibilities.

2.1.2 Five essential characteristics

In order to deduce exactly what is part of cloud computing, a list of five characteristics have been defined by the National Institute of Standards and Technology (NIST).The five characteristics of the cloud computing model have since been refined numerous times by experts and consist of the following:

- **On-demand capabilities:** This characteristic can be seen as service based, thus allowing a consumer to easily configure computing resources individually, without filling out forms or requiring human interaction with each service provider. This is mostly done through a web-based self-service portal or management console.
- **Broad network access:** Through a simple online access point, consumers can access cloud capabilities over the network through standard mechanisms anywhere and anytime using any devices (smartphones, tablets, laptops, and office computers).

- **Resource pooling:** Computing resources are pooled together to serve multiple consumers. These resources use a multiple-tenant model, with different physical and virtual resources being assigned and reassigned according to the consumers' demand in a dynamic way (ISACA, 2012). The cloud service provider manages all of its resources and allocates them between the consumers. Resources include storage, processing, memory and network bandwidth among others.
- **Rapid elasticity:** The cloud is flexible and scalable to suit the (changing) business needs. Resources are provisioned and released on demand, making sure that business applications will have the exact amount of capacity needed at any point in time. This characteristic allows capabilities to scale rapidly inward and outward commensurate with consumers' demand.
- **Measured service:** The amount of resources used by a consumer can be monitored, measured, controlled and reported from both the consumer and cloud provider's side, providing transparency.

There is one more characteristic that is not included in the NIST cloud computing model, but is highly advocated by the Cloud Security Alliance. This characteristic is called 'multi tenacity' (Cloud Security Alliance, 2011). This implies the use of the same resources by multiple consumers. The consumer could be a business unit or a distinct organization, but would still share infrastructure in order to utilize cloud service offerings, requiring well defined segmentation models. With multi-tenancy this could mean that users will be able to see residual data or trace of operations by other users. This means that there is a need for a well-established policy-driven enforcement and isolation for different consumers.

2.1.3 Deployment models

The cloud deployment models are a form of categorization of the cloud environment, distinguishing the different deployment models by proprietorship, access and size. Deployment models give consumers a view of the nature and purpose of cloud computing. Different cloud models fit with different requirements. There are four cloud computing deployment models as defined by the National Institute of Standards and Technology (NIST), namely:

- **Public cloud:** In this type of deployment model, cloud services are delivered over a network and is available for use by the general public. Service and infrastructure are provided to various consumers and consumers do not have any distinguishability and control over the location of the cloud infrastructure. The cloud infrastructure exists on the premise of the cloud provider (Mell & Grance, 2011)
- **Private cloud:** This type of deployment model is available only to users within a single organization (comprising multiple consumers e.g. business units) (Mell & Grance, 2011). It is the responsibility of the consumer to ensure the servers are accessible through the internet and only authorized employees have access to the servers and network.
- **Community cloud:** In this type of deployment model the setup is provisioned for exclusive use by and mutually shared between many consumers that belong to particular community. Community cloud can exist on or of premises and may be owned by either a third party or one or more of the consumers in the community (Mell & Grance, 2011).
- **Hybrid cloud:** This deployment model is integrated. The cloud infrastructure is an arrangement of two or more of the aforementioned cloud infrastructures (private, public or community).

This research is interested in the impact of a client's migration to a cloud computing environment and its subsequent effects on the IT audit. To be able to explore this further, focus is put on a group of cloud computing security risks (data integrity) and how this has affected the consumer. Further investigations will be made with regards to public cloud only. This choice has been made, since public cloud is the most popular form of cloud deployment models and encompasses a variety of inherent security risks that need to be considered.

2.1.4 Service models

There are various ways a cloud computing based service is consumed and utilized. Service models can be actualized as any of the deployment models available in cloud computing and require important considerations from the consumer. From the definition of the cloud computing model, as postulated by the National Institute of Standards and Technology there are three different approaches to cloud-based services:

- **Software as a Service (SaaS):** The only capability the consumer has is to utilize the provider's applications running on the cloud environment, meaning the consumer has no control and does not manage the underlying cloud infrastructure. However, there is a possible exception of limited user-specific application configuration settings such as (limited) administrative settings and preference selections (Mell & Grance, 2011). Considering the consumer has no control over the cloud infrastructure, it is the responsibility of the cloud provider to carry out security operations and other provisions. SaaS provides consumers with the capability to run applications already hosted on the cloud infrastructure and thus removes the need to install and run applications on private computers or data centers. This reduces the total cost of maintenance, hardware and software development, as well as eliminating the expense of software licensing, installation and support.

- **Platform as a Service (PaaS):** Depending on the programming languages, libraries, tools and services supported by the cloud provider, consumers have the capability to deploy their own developed or acquired applications onto the cloud infrastructure. PaaS turns the cloud computing platform into an on-demand service upon which consumers can develop and deploy applications. The cloud provider delivers the hardware and software tools needed for application development, allowing consumers more control over applications and configuration settings. The PaaS service model reduces the cost and complexity of buying, operating and maintenance of the hardware and software components of the cloud infrastructure, but provides more responsibility to the consumer. This means that the responsibility of security operations and protection is split between the provider and consumer.
- **Infrastructure as a Service:** This service model provides the basic infrastructure of servers, software and network tools as an on-demand service, allowing consumers to develop and deploy their applications with the broad freedom to choose between which of the many environments and operating systems is to be hosted (Mell & Grance, 2011). Consumers have the capabilities for not only the processing, but also fundamental cloud resources including storage and networks. IaaS avoids the purchase, housing and management of basic hardware and software infrastructure components and instead provides them as virtualized objects to consumers. With this broad freedom consumers have the full responsibility for security operations, outside of some of the minor infrastructure security operations (i.e. network, firewall) which fall under the providers control.

Depending on the service model there will be differences in the scope and control of consumers and cloud providers. In order to clarify, figure 3 breaks down the responsibilities of the consumer and provider from the traditional solution (on-premises) to a complete SaaS service model.

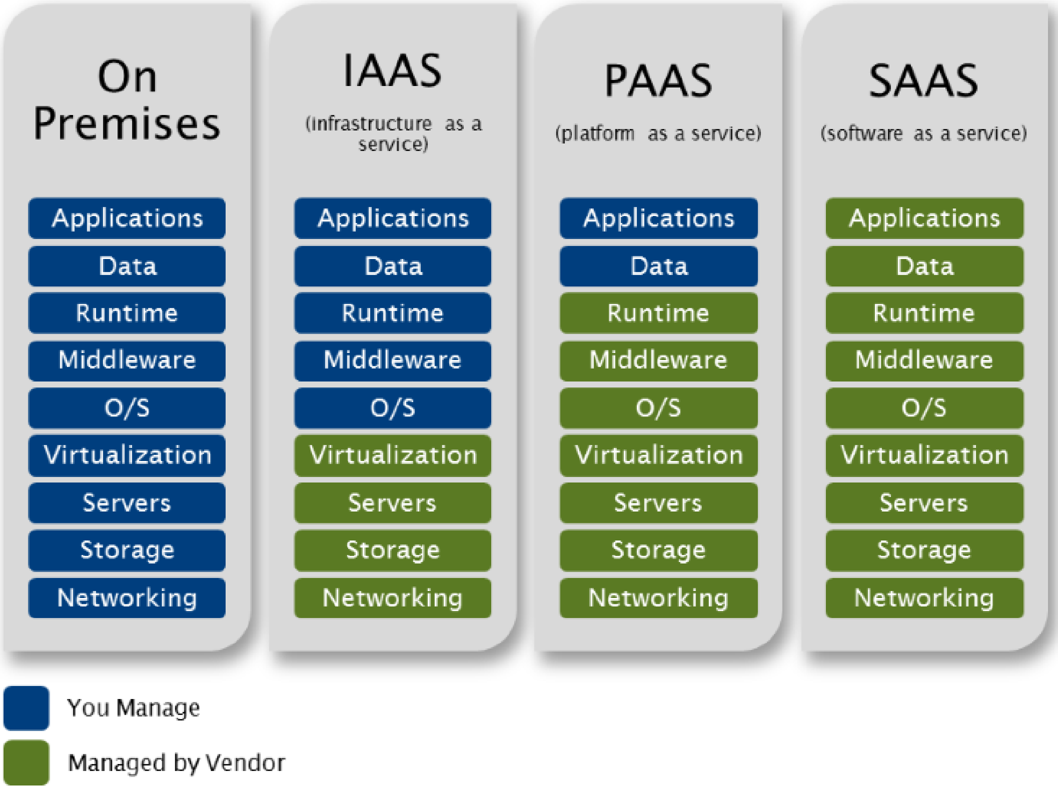

Figure 3: Breakdown of the cloud service model responsibilities (Arruda, 2015, para. 3)

To narrow the research even further, focus within public cloud will be put on the SaaS service model only. When comparing cloud service models, SaaS is and continues to be the most dominant form with 45 percent[3] of cloud implementation being SaaS (Cisco Global Cloud Index, 2015). Being the most dominant form, it is of great interest to this research to clarify the effects of data integrity risks on this service model and what this means for the IT audit.

[3] According to the study performed by Cisco Global Cloud Index (2015), PaaS implementations count for 42 percent of all cloud implementations and IaaS counting for only 11 percent. It is predicted that SaaS will increase to 59 percent by 2019 *(Cisco Global Cloud Index, 2015)*.

2.2 Advantages and constraints

Businesses can reap benefits from a migration to a cloud environment. However, it is not without its downsides. With the many cloud computing advantages, come some drawbacks as well. The following two lists have been constructed through a literature study (Armbrust, et al., 2010; Grossman, 2009; Wang & Chang, 2016). Table 1 shows the reported advantages and the sources they were collected from. Respectively, table 2 shows the reported disadvantages and the sources they were collected from.

Reported advantages of cloud computing:

1. **Cost savings:** No matter the size or type, businesses' main goal is to earn money while keeping expenses to a minimum. With the provision of unlimited cloud resources and the lack of in-house server storage and on premise infrastructure, capital costs are reduced substantially. Having applications and data on the cloud subsequently reduces associated operational costs such as development costs of in-house developed systems, maintenance and administration costs.
2. **Reliability (dependability):** Applications can be accessed through any device with an internet connection. Since, cloud computing uses massive pools of IT resources and a quick failover mechanism – if one server fails, hosted applications, services and data can easily be carried over to any other servers.
3. **Scalability:** This is a built-in feature for cloud computing deployments and virtualization. The cloud computing environment acts as an adaptive infrastructure which can be shared by different consumers (multi tenacity). This flexibility allows for computing resources to be balanced on demand as more consumers join the cloud environment or as consumers' requirements change over time. The process of adding additional computing capacity is almost as simple as adding building blocks to an existing grid (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011). Additionally, scalability contributes to the reduction of server and capacity costs.
4. **Shorter implementation time:** Cloud computing provides the necessary hardware and software resources at the needed capacity in near real time (ISACA, 2011). Leading to a faster time to market in many businesses and making new classes of applications possible and deliver services that were not possible before.

Reported advantages	References (sources)
Cost savings	(Armbrust, et al., 2010; Grossman, 2009; Wang & Chang, 2016; Hayes, 2008)
Reliability (dependability)	(Armbrust, et al., 2010; Grossman, 2009; Wang & Chang, 2016; Hayes, 2008)
Scalability	(Armbrust, et al., 2010; Grossman, 2009; Wang & Chang, 2016; Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011)
Shorter implementation time	(Armbrust, et al., 2010; Grossman, 2009; Wang & Chang, 2016; ISACA, 2011)

Table 1: Reported advantages and references.

Reported disadvantages of cloud computing:

1. **Vendor Lock in:** Switching cloud services is not something that has yet completely evolved, although cloud providers promise that the cloud is flexible and easy to integrate. Once a consumer chooses a cloud provider, it will become clear how difficult it is to migrate their services to another vendor. Currently hosted and integrated applications on one platform may throw up errors of interoperability and other issues on another platform.
2. **Limited control:** Consumers have limited control over their applications, data and services, since the cloud infrastructure is entirely owned, monitored and managed by the cloud provider. Additionally, limited control could lead to transparency and ownership issues. A cloud provider can also perform updates and patches that could have an effect on the consumer's applications, regulations or monitoring without the consumer having any influence.
3. **Downtime:** It is important for the consumer to consider how dependent their business would be on the reliability of the network and cloud computing. Cloud computing makes businesses dependent on the reliability of the network access. When it is offline, the business applications will be offline too. A small outage, although harmless at first sight, can cause great damage to businesses' operations and public image. Since a small outage will hinder customers' access to the cloud consumer's services. As described by CRN on cloud computing outages in 2015, even the most reliable cloud computing providers suffer from server outages now and then (Tsidulko, 2015).
4. **Data security and privacy:** When it comes to cloud computing, data security is the

biggest concern, since cloud computing can enlarge existing risks to a certain degree. By leveraging business applications and services to a cloud computing based infrastructure, consumers are essentially giving away control over private data and information that might be considered confidential. Leading to a loss of control by the consumers. Thus, the cloud provider's reliability is critical, as it is the responsibility of the cloud provider to manage, protect and retain the sensitive data. The following paragraph will further elaborate on cloud computing risks.

Reported disadvantages	References (sources)
Vendor Lock in	(Armbrust, et al., 2010; Grossman, 2009; Wang & Chang, 2016; Kaliski & Pauley, 2010)
Limited control	(Armbrust, et al., 2010; Grossman, 2009; Wang & Chang, 2016; Sengupta, Kaulgud, & Sharma, 2011)
Downtime	(Armbrust, et al., 2010; Grossman, 2009; Wang & Chang, 2016; Tsidulko, 2015)
Data security and privacy	(Armbrust, et al., 2010; Grossman, 2009; Wang & Chang, 2016; Sengupta, Kaulgud, & Sharma, 2011)

Table 2: Reported disadvantages and references.

2.3 Risks

Risks within cloud computing can be seen as a double edged sword. This can be reflected in the behavior of organizations that are planning a migration in the near future. Information security is stated as their major concern and attracts a lot of attention. According to 44 U.S.C., Section 3542 (2002) information security is defined as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction" (p. H. R. 2458-49.) in order to provide three essential quality aspects, namely confidentiality, availability and integrity, which can be categorized by a security triad

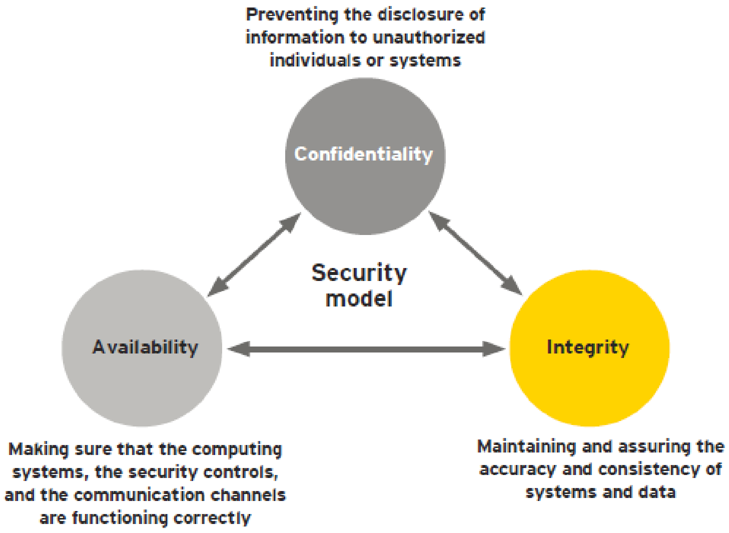
Preventing the disclosure of information to unauthorized individuals or systems
Confidentiality
Security model
Availability
Integrity
Making sure that the computing systems, the security controls, and the communication channels are functioning correctly
Maintaining and assuring the accuracy and consistency of systems and data

Figure 4: Security triad with the pillars of information security *(EY, 2014, p. 5)*

(Concrad, Misenar, & Feldman, 2010), as can be seen in figure 4. This research is focused on the information integrity aspect and to put it more precisely: focus is on data integrity[4]. Information integrity is defined as representational faithfulness, meaning that under this representational view the information corresponds to what is actually being represented i.e. the so called business reality (Christiaanse & Hulstijn, 2011). The minimum criteria that must be satisfied, in order to judge whether given information sets possess representational faithfulness are the core attributes: completeness, timeliness, accuracy and validity (Boritz, 2005). Information integrity requires data integrity: “the accuracy and consistency of stored data, in absence of any alteration to the data between two updates of a file or record” (Rathod & Sapkal, 2014, p. 288).

Through an online literature study research[5] (Cloud Security Alliance, 2016; Chou, 2015; Mell & Grance, 2011; ENISA, 2009) and “water cooler”[6] conversations a list of cloud computing risks has been formulated, see table 3. Below, the risks are described and the service models that are affected by the risks are highlighted in yellow. These risks are not distinct but do show overlap to some degree.

Table 3: Cloud computing risks

Risk	Description	Affected service models
Data breaches	An incident in which an individual who is not authorized releases, views or steals confidential, sensitive or protected information (Cloud Security Alliance, 2016). While data breaches are not specific to cloud computing environments, they do become an attractive target due to the vast amount of data stored on cloud servers and high accessibility and ubiquity. Data breaches can happen trough targeted attacks or simply caused by human error or application deficiencies such as a multitenant cloud service database that is not properly designed. Data breaches can also result from insider threats, through malicious employees.	IaaS PaaS SaaS

[4] Data integrity does not equal information integrity. Instead information integrity requires data integrity (Boritz, 2005).

[5] The literature study research depended on existing relevant literature, found through available sources such as Tilburg University, complemented by Google Scholar. The search terms: “cloud computing risks”, “cloud security issues” and “cloud security threats” were used.

[6] “water cooler” conversations are considered informal conversations taking place throughout the work environment leading to rich information sharing and increased opportunity for organizational learning *(Waring & Bishop, 2003)*.

Data loss/leakage	The prospect of permanently losing organizational data. Data loss can not only be caused by data breaches and malicious attackers, but it could also be due to accidental deletions by the provider, natural and business disruptions or even due to a consumers losing encryption keys (Cloud Security Alliance, 2016).	IaaS PaaS SaaS
Account or service hijacking	Attack methods such as phishing, exploitation of vulnerabilities (hardware and software) and fraud. Cloud computing amplifies the impact of these attacks by making it possible for attackers to eavesdrop on activities and transactions once they have access to the credentials (Cloud Security Alliance, 2016). Furthermore, this allows them to manipulate data and return adjusted false information. Alternatively, once an exploiter has access to one consumer's data, the exploiter could run exploitation scripts affecting other consumers on the same cloud server or even providing the exploiter access to other consumers' data.	IaaS PaaS SaaS
Insecure interfaces and APIs	Cloud providers expose a set of software interfaces or APIs (application programming interfaces) allowing consumers to manage and interact with cloud services including cloud provisioning and monitoring (Cloud Security Alliance, 2016). From authentication and access control to monitoring, user operations and encryption, the APIs should protect against accidental and malicious attempts of circumvention. An insecure API will lead to inflexible access controls or improper authorizations, allowing exploiters access to consumers' data and applications harming confidentiality, integrity, availability and accountability.	IaaS PaaS SaaS
Malicious insider	This threat has many faces: a current or former employee, a system administrator or a business partner. The malicious agenda by the insider ranges from data theft to revenge and in a worst case scenario a determined insider can destroy whole infrastructures or manipulate data. Organizations that solely depend on the provider for security are at a great risk, since providers may not reveal how it allows its employees access to the assets (physical or virtual) or how it monitors these employees.	IaaS PaaS SaaS
Limited technology knowledge	Unknown exposers due to the absence of knowledge regarding versions of software, code update, security design or compliance of the internal security procedures, patching and monitoring. These exposures and information regarding who is sharing your infrastructure are relevant to understanding the company's security posture in a cloud environment.	IaaS PaaS SaaS
Cloud abuse	This risk is more of an issue for the provider than for cloud consumers. Due to the weak registration systems, the facilitated anonymity and limitations of fraud detection capabilities. Spammers and malicious coders are able to conduct criminal activities (such as DDoS attacks , key cracking or propagating malware) with the support of the unlimited computing power of cloud environments. Consumer could indirectly be affected by service availability issues and data loss.	IaaS PaaS SaaS

Shared technology issues	Cloud providers share infrastructure, applications and platforms. If there is a vulnerability or misconfiguration in any of these layers, it could possibly affect the other consumers. This is a form of single point of failure and is undesirable in cloud computing, since it compromises the availability and reliability of the systems.	IaaS PaaS SaaS

While some of these risks could be applied to traditional settings, cloud computing has enlarged them to a certain degree. Through semi-structured interviews with IT auditors at EY, it came out that these risks could indeed have a big impact on data integrity. These short interviews concerned IT auditors who have worked with clients that use cloud computing. The context of the interviews was mainly concerned with the IT auditors experiences with clients using cloud computing and what possible security risks could have an impact on data integrity, in their respective views. Additionally, during the interviews their views and expectations on cloud computing with regards to the IT audit was further discussed. The table of risks is to be further investigated with regards to the risks' effects on data integrity and how this influences the IT audit.

This chapter has introduced cloud computing and the different deployment and service models. The advantages and disadvantages have been listed, and cloud computing risks were investigated. This research will further only take public cloud into consideration, as it is the most popular form of cloud deployment model and encompasses a variety of inherent security risks. Within the public cloud, this research focusses on the SaaS service model as this is the most dominant form of cloud implementation. Additionally, the table of cloud computing risks will be further investigated.

3. IT audit and methodology

According to Sarbanes-Oxley Act Section 404, organizations which are listed with the United States Securities and Exchange Commission to trade on any US based stock exchange are required to include information regarding the scope and adequacy of the internal control structures and procedures for the financial reporting when they publish their annual report (Soxlaw, 2006). This is one of the many reasons why audits are conducted. An audit can be interpreted as controlling and reporting on an organization, with the goal of providing independent assurance and evaluation of the financial statements of organizations. This is done in order to have a reliable and accurate representation of the transactions they claim to represent (EY, 2016c). The objective of the audit is to obtain reasonable assurance about whether the financial statements of an organization is free of misstatements due to fraud or error. This will further lead to an opinion (by the auditor) on whether the financial statements are in accordance with an applicable financial reporting framework (Knechel & Salterio, 2016). Accordingly, the auditor will attest to and report on the assessment in order to provide assurance to the management of an audit client and third parties. This chapter consists of two parts, with the first paragraph treating the position of the IT audit within the audit. Subsequently, the second paragraph will delve into the methodology applied within EY, starting with a clarification of the IT audit terminologies followed by a depiction of the IT audit process. Additionally, providing a background on data integrity and the IT audit in cloud computing.

3.1 IT auditing within the audit

IT audits are a process of examination of the management and internal controls within an IT infrastructure. IT audits were formerly called ‘electronic data processing audits’ (EDP) and according to Hansen and Messier (1982) EDP auditing consisted of a collection of activities used by the IT auditor to conclude whether reliance could be put on the systems and whether there was a correct production of data output. A much more recent and clear definition is made by Van Praat and Suerink (2004) in which they define it as the discipline that deals with the assessment and advisory on objects (of information provisions and services) in an automated environment. The goal of the EDP auditing is to help organizations both qualitatively and quantitatively, in order to realize the client’s objectives (Van Praat & Suerink, 2004).

The IT audit can also be seen as the process of collecting and assessing evidence of the information systems (IS), procedures and operations of an organization. Subsequently, the collected evidence will be evaluated in order for the IT auditor to come to a formal opinion of the effectiveness of controls and safeguarding assets that maintain data integrity and operation effectiveness (Tucker, 2001).

The IT audit differs from the financial audit in various aspects. The purpose of financial audits is the evaluation of whether organizations are complying with standard accounting practices is one of those aspects. Instead, IT audits are focused on determining risks related to information systems and the evaluation of the system's internal control design and effectiveness. The IT audit process consist of several steps. The first being the process of gathering information and understanding the business environment and the entity's use of IT. Next, is the scoping to determine which IT applications are relevant to the audit (including, the understanding of involved risks). Subsequently, the audit strategy is determined for the relevant IT applications. Then, the risks are identified and evidence is gathered and assessed. Finally, the last step consists of performing evaluations, gaining an understanding and formulating an opinion of the existing internal controls. As part of the audit engagement, systems in place will have been assessed and evaluated on quality and the concerns: confidentiality, integrity and availability (CIA). The former concerning authorized use and access, integrity focusing on the accuracy and completeness of data and the latter covering system's uptime measurements. For example, who has access to the applications and hardware? Have applications or systems changed and has this change been taken into consideration with regards to the organization's data processes? Who has access to the data and are they authorized to delete and make changes to the data? Who reviews these changes to the data to confirm that all changes were indeed authorized.

The IT auditor will finally make a professional judgement on whether reliance can be put on the IT processes in place in an organization. This IT audit process is to be further clarified in paragraph 3.2.2.

3.2 EY audit methodology

The methodology applied at EY is the EY Global Audit Methodology (EY GAM), which is similar to the methods used by the other Big Four companies. EY GAM provides the auditors with a global framework for applying a consistent thought process to all audits (EY, 2016d). The provision of a global framework makes EY GAM applicable to all audits, while still providing a number of specific approaches tailored for audits of certain types of entities.

The audit teams are supported by instructions and IT tools to make more efficient audits possible. While different commercial and internally developed applications are applied, it is the audit software EY Canvas that makes sure that the global audit methodology (GAM) is being applied consistently, efficiently and that the audit procedures are well documented (EY, 2016e). EY Canvas provides the auditors access to auditing standards, guidance and reference materials. In practice, this means that whenever an audit aspect, such as cloud risks, is not supported by EY Canvas, it will often be overlooked.

3.2.1 IT audit terminology

Before proceeding with the IT audit procedure, it is best to clarify some general IT audit terminology.

Information produced by the Entity (IPE)
Organizations being audited use IT applications in order to collect, process and store data as relevant information output to reports or data files. This output is called IPE. IPE can be defined as any information created by the organization by either using IT applications, end user computing tools (i.e. Microsoft Access, Excel, and Word) or any other means (i.e. manual preparation of information) (EY, 2016g). Much of this information is relevant and used in the performed audits. IPE is used by the organizations in the performance of controls and needs to be sufficiently complete and accurate.

IT General Controls (ITGC)
ITGCs are controls applied to all system components, processes and data for organizations or IT environments, with the capability covering identification, evaluation and validation of controls. ITGCs support the continued functioning of applications and IT-dependent manual

controls supporting the production of accurate information (EY, 2016f). Objectives include integrity of programs and data files, as well as proper implementation of applications.

Significant class of transactions (SCOT)

SCOTs consist of classes of transactions that materially affect a significant account, which are relevant accounts for the financial statements. SCOTs can be identified as those classes of transactions that result in the amounts recorded in a significant account (EY, 2016h). An auditor obtains an understanding of the SCOTs in order to identify risks of material misstatements affecting the accounts. Through the identification of so called WCGWs (what can go wrong), the auditor is assisted in determining the nature, timing and extent of the further audit procedures. The risks of material misstatements that could possibly occur within a SCOT are described through WCGWs and could help in reducing the IT auditor's detection risk. Blokdijk (2004) defines 'detection risk' as "the risk that an auditor's substantive procedures will not detect a misstatement that exists in an account balance or class of transactions that could be material, individually or when aggregated with misstatements in other balances or classes" (p.187). The WCGWs help the IT auditor to assess and determine the amount of required audit work in order to reduce the IT auditor's detection risk to an acceptable degree (Blokdijk, 2004).

Controls

A major part of the work of an auditor consists of testing controls. Controls are tested in order to evaluate the operating effectiveness of controls over the SCOTs and significant disclosure processes (EY, 2016i). Besides the ITGCs, in order to evaluate the effectiveness of controls, the following controls are also tested:

- **Manual controls:** A manual control that is performed outside of a system by certain individuals, i.e. a manager reviewing a document and signing it.
- **IT dependent manual controls:** Manual controls (usually detect and correct controls) that require some degree of IT involvement, i.e. a particular system generating a report which requires a manager to review it and perform some action.
- **Application controls:** fully automated controls, with some degree of human interaction if needed. Application controls may be system configuration settings, i.e. a particular system disabling and locking out after three wrong password attempts by an user.

In figure 5 the aforementioned controls are categorized by type and objectives.

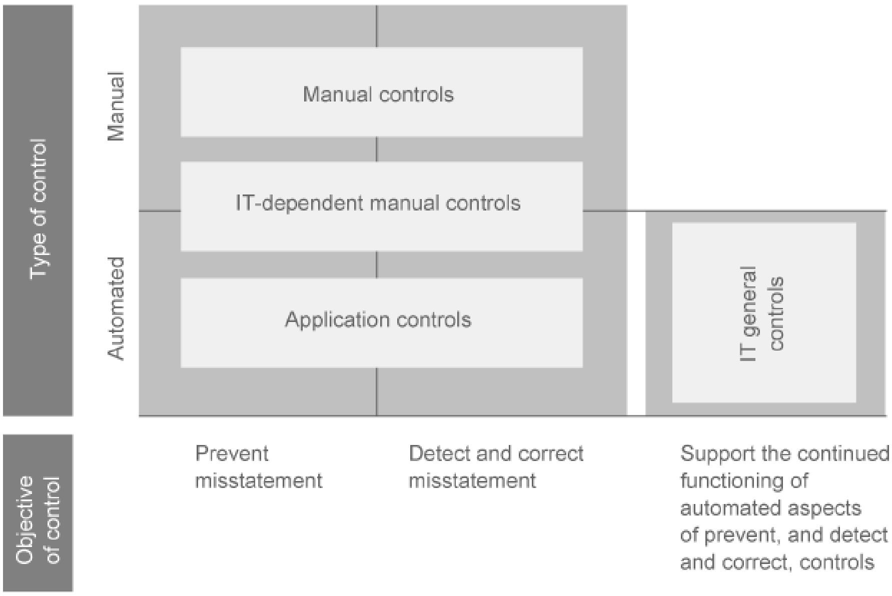
Type of control
Manual
Automated
Manual controls
IT-dependent manual controls
Application controls
IT general controls
Objective of control
Prevent misstatement
Detect and correct misstatement
Support the continued functioning of automated aspects of prevent, and detect and correct, controls

Figure 5: relevant controls categorized by type and their objectives *(EY, 2016i, para.. 1).*

3.2.2 IT audit procedure

Performing effective and efficient audits requires a clear understanding of the business and the role of IT and its use by the entity. IT is ingrained in business and financial operations and takes many forms. Entities use IT applications in the processing of SCOTs, i.e. transactions processing and recording. The relevant IT applications for the audit are those that generate IPEs and support the application and IT dependent manual controls. Obtaining an initial understanding of the use of IT and the complexity of the IT environment of an entity, provides the auditor with an understanding of the business and how the entity operates. This antedates the audit strategy selection.

After gaining an understanding of the entity and the way IT is used by the entity, the auditor will make scoping decisions to determine which IT applications are relevant to the audit. From the relevant IT applications the auditor will reach an understanding of the risks involved in the use of the IT applications and the IT processes (manage change, manage access and manage IT operations). The manage change process has the objective of making changes to IT application programs and other IT environment components that are appropriate and function as they are supposed to. The risks involved are assessed as for changes to the IT applications, which requires understanding of the processes. Manage Access has the objective of providing access to the IT applications, data and IT environment only to authorized users and restricting them to perform only authorized actions. In order to obtain an understanding of the authentication paths for each user, the IT auditor needs to identify the key points at which users are authenticated to the IT applications and other IT environment components. Manage IT operations has the objective of providing a reliable processing environment that is prepared for operation issues and other disruptions. This involved backups and business continuity plans.

Understanding of the aforementioned risks in IT application and IT processes, allows the auditor to make a professional judgment on whether reliance can be put on the IT processes in place. The audit strategy depends on whether the auditor plans to rely on the related IT processes.

When the auditor plans to rely on the related IT processes, the strategies can be:

- **ITGC-reliance strategy:** understanding the IT processes and the risks within the processes, followed by the identification and testing of ITGCs that the entity has in place to address these risks (EY, 2016j). Understanding of the design of the ITGCs and their implementation is confirmed through a combination of walkthroughs and other procedures, i.e. inquiries and inspections. Finally, the auditor will make an evaluation of the effectiveness of the relevant ITGCs.
- **IT-substantive strategy:** In order to provide reasonable assurance, the IT auditor starts with understanding the IT processes and the risks within the processes, followed by substantive testing of the IT process activities in order to address these risks (EY, 2016j). With this strategy, the auditor designs IT-substantive procedures to address the risks within the related IT processes and subsequently reducing the risk to an acceptably low level.

When the auditor does not plan to rely on the related IT processes, the strategies can be:

- **Direct testing of application and ITDM controls and substantive testing of IPE[7]:** The auditor tests application and ITDM controls throughout the period, to come to an understanding and determine if the risks have resulted in an error in the processing (EY, 2016j).

[7] The IT auditor will still assess the design of the processes from which this is obtained.

- **Substantive only strategy[8]:** the auditor does not rely on controls over SCOTs. Substantive procedures are designed and performed at the assertion level[9] in order to address the risk of material misstatements (EY, 2016j). Whenever material misstatements are identified at the assertion level, their effects will be quantified in the financial statements.

3.2.3 Data integrity

In section 2.3, information integrity was mentioned as being representational faithfulness with the minimum criteria that must be satisfied, in order to judge whether information sets possess representational faithfulness being the core attributes: completeness, timeliness, accuracy and validity (Boritz, 2005). Information integrity requires data integrity, which is concerned with "preserving the meaning of information, preserving the completeness and consistency of its representations within the system, and with its correspondence to its representations external to the system" (Mayfield, Roskos, Welke, & Boone, 1991, p. 6).

Mayfield et al. (1991) have set up three goals for data integrity:

1. Prevention of unauthorized users from making modifications.
2. Maintaining the internal and external consistency of data.
3. Prevention of authorized users from making improper modifications (p. 8).

None of these goals however are able to be achieved with full certainty and may require other supplemental risk reduction procedures.

The IT audit is traditionally focused on the annual audit making sure that the financial statements are reported accurately and do not contain misstatement. To be able to achieve this and to provide assurance to the clients, IT audits are performed to test controls and mitigate information risks. Transactions are an important part of every business. An important aspect of the IT auditor's activities is obtaining an understanding of the SCOTs in order to identify risks of material misstatements affecting the accounts. As mentioned in section 3.2.1, a SCOT is a significant class of transaction: every important transaction that materially affects a significant account and thus considered relevant for the financial statement. A major part of

[8] Even then the IT auditor still needs to assess the reliability of the evidence.

[9] An assertion is a statement that is given as an absolute fact. The assertion level is the level at which management presents financial statements as an absolute fact, meaning it shows the true valuation of inventory.

the work of an auditor consists of testing controls. Controls are tested in order to evaluate the operating effectiveness of controls over the SCOTs and significant disclosure processes. Additionally, it is important that the IPEs, which are used by the entity in the performance of controls, are sufficiently complete and accurate. Clients need to have the right controls in place that mitigate risks and prevent misstatements that could affect the data integrity. This means that clients need to have constraints in place that prevent certain actions or force certain procedures. For example, a date of birth should always be set before the present date, or a primary key cannot be set at the value null in a database table.

The Clark and Wilson model is an integrity policy model with the goal of ensuring integrity of data to prevent fraud and errors. There are two key aspects to the Clark and Wilson model: firstly, to ensure that data is not manipulated arbitrarily by users, but only through well-formed transactions; and secondly, that there is segregation of duty in place (Clark & Wilson, 1987). In order to have well-formed transactions, it must be ensured that the data items can only be modified by a certain set of programs. For these programs it must be ensured that they are controlled for proper construction and that there are controls in place that ensure their continued validity (Clark & Wilson, 1987). For the separation of duty, it must be ensured that the users can only use a certain set of programs and that this again is inspected to ensure that they are reliable.

Two important procedures have been put in place in the Clark and Wilson model: the integrity verification procedure (IVP) and the transformation procedure (TP). The IVP is responsible for verifying that the data set is well-formed, thus making sure that the required integrity constraints are in place. The TP makes sure that newly entered data meets the applicable integrity constraints and that for all transformations that are made, it is guaranteed that the data stays well-

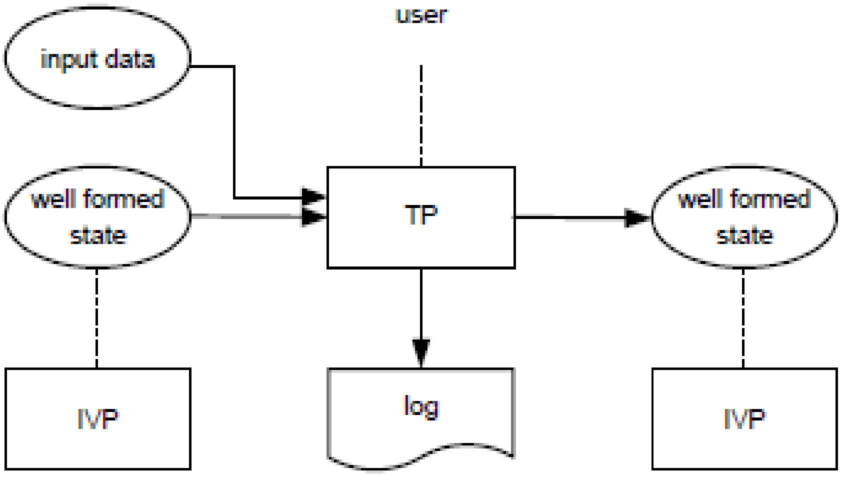

Figure 6: The integrity policy of the Clark and Wilson model *(Christiaanse & Hulstijn, 2011, p. 3).*

formed and that the integrity constraints are maintained. The integrity policies as set in the Clark and Wilson model can be seen in figure 6. In figure 6, the arrows are considered information flows and the dashed lines represent control (Christiaanse & Hulstijn, 2011).

As mentioned before, it is important that the transactions stay well-formed. Change management is an important aspect in this case, since it is important that new software and changes are inspected in order to ensure that data integrity is maintained.

Outsourcing to cloud is a rising trend and this increases the difficulty for users to effectively verify the data management of the cloud provider, ensuring that the data is being handled effectively on the cloud servers (Al Saiyd & Sail, 2013). It is not only possible that the cloud service provider could accidentally or deliberately alter or even delete information from the cloud server, but it is also harder for the clients to keep track of changes and modifications made to applications and servers. Looking at the Clark and Wilson model in the cloud, the two aspects of the integrity policy model will be different. It is harder for the clients to ensure that the cloud provider has effective controls in place and that the IVP and TP are adequately performed. Additionally, it may be unclear how the cloud provider takes care of segregation of duties and whether the right integrity constraints are enforced. Looking at change management, which also affects the Clark and Wilson model, it may be harder for the client to keep track of the changes and updates enrolled on the servers and applications by the cloud provider.

This research is interested in what the effects are of the security risks of section 2.3 on the data integrity of organizations both on the cloud and in traditional structures. Subsequently, investigating the effects it has on the IT audit. Additionally, it is of interest what the cloud means for the Clark and Wilson model, and how this affects the data integrity. This will allow this research to draw a conclusion regarding the impact of an organization’s migration to a cloud environment and its effects on the IT audit.

3.2.4 IT audit in cloud computing

A decision to migrate to a cloud environment is not a decision that should be taken lightly by an entity’s management. Organizations should be well informed in the risks and implications involved in cloud computing and a clear vision should have been established of what they want to accomplish in terms of where they are going. Well informed organizations should conduct due diligence and design adequate measures and mitigation strategies to manage the associated risks and challenges of cloud computing. Additionally, IT auditors will need access to the provider's servers and systems. However that is not always guaranteed or even allowed in the contract between client and cloud provider.

Cloud computing services have the capability of being rapidly deployed. This does not only make them attractive, but also signifies the importance of considerations regarding the impact on change management. Often, the effects of cloud computing on an entity's internal controls are overlooked. This can partially be blamed on the easy deployment and modification of applications in the cloud and due to the cloud services being procured outside the entity's departments. Cloud computing however transforms a business. The introduction of new technologies and systems requires an entity to reorganize its databases and transfer data from "old" legacy systems to new cloud environments. Subsequently, new risks are introduced and traditional security risks are enlarged to a certain degree.

Insecure data and data integrity vulnerabilities have an effect on the IPEs collected by the IT auditor during the audit process of an organization's IT applications and IT processes. IPEs are used by the organization in the performance of controls and need to be sufficiently complete and accurate. IPEs that could possibly be considered unreliable, containing inaccurate and incomplete data can hinder the IT audit process or worse the IT auditor will have nothing to rely on.

This thesis investigates the table of cloud security risks as mentioned in section 2.3, how it affects the entity's data integrity, what their influence is on the IPEs and their impact on cloud computing. Additionally, this research will study what ITGCs, entities have taken into consideration and implemented in order to mitigate these risks. This means that this research will further investigate the ITGC-reliance strategy and leave the other IT audit strategies out of this research.

With a migration to cloud, the client cedes control over its applications and data to the cloud provider. As mentioned in section 2.1.1, the assignment of responsibilities between the cloud provider and the client has become more complex in cloud computing (Julisch & Hall, 2010). This is due to the numerous possible configurations, deployments and service models and the extent of controls that can be put in place. This signifies the importance of clear agreements between the client and the cloud provider with regards to responsibilities. In traditional settings, all the responsibilities lie with the client with regards to controls and security. However, with a migration to cloud this role is starting to change from execution to a direction role. In this new setting, the client informs the cloud provider what needs to be done, what degree of security is required and that they are provided with a reasonable degree of assurance.

With regards to the role of the IT auditor, it also will be affected by a client's migration to cloud computing. At a traditional setting, the IT auditor is responsible for the testing of controls and procedures at the client. Additionally, it is the responsibility of the client to have the right security controls in place in a traditional setting. However, when it comes to cloud computing, it will be the cloud provider who is responsible that the servers are continuously maintained, running and that there are efficient controls in place in order to provide the client with reasonable assurance. The cloud provider needs to make sure that an audit is performed at their setting, which is recorded in an assurance report that is then provided to their clients. The IT auditor's duties will change from the actual testing of controls to the investigation of irregularities in the assurance report. The audit procedures of the IT auditor will become a more judgement and professional skepticism approach with regards to the assurance report and agreements between the client and cloud provider (Chan & Vasarhelyi, 2011).

From the literature study on cloud computing in chapter two and the literature study on the IT audit in the present chapter, this research formulates two expectations to be tested in the cases in the following chapters. The two expectations are related to the changing role of the client and the IT auditor. The two expectations are defined as follows:

1. The client will shift from an execution role to a direction role, with regards on what needs to be done (Julisch & Hall, 2010).
2. The IT auditor will shift from actual testing at the client, to a more judgement and review of the assurance report (Chan & Vasarhelyi, 2011).

This chapter introduced IT audit and the EY GAM methodology. General IT audit terminologies have been elucidated and the auditors' audit procedures from understanding the business to the different audit strategies have been clarified. This chapter concludes the theoretical part of this report having provided a sufficient theoretical background to the topics of cloud computing and IT audit. The following chapters will delve into the practical side of this research starting with an explanation of the research methodology and case descriptions.

4. Research methodology

This chapter elaborates on the chosen methodology as performed by this study. The first paragraph delves into the research process and explains the action research approach, elaborating on the methodology and the steps in this research. Subsequently, paragraph two will give a description of the chosen case companies, applications, interviews and interviewees. Finally, paragraph three will provide a description of the research setting at EY.

4.1 Research process

As has been stated in section 1.4, this research study consists of a theoretical and empirical part in order to have the optimum capability of answering the main research question. From the conceptual model, it became clear what this study included. Namely studying how organizations are affected by data integrity risks after they have migrated to a cloud environment and how this subsequently affects the IT audit.

To be able to study these effects and finding an answer to the main research question, three sub-questions were introduced, as has been outlined in section 1.3. In order to have an all-inclusive research, each sub-question puts focus on a different part of this research. The first sub-question focused on cloud computing and its risks, clearly defining what cloud computing is and what its advantages, disadvantages and relevant risks are. The second sub-question was focused on the IT audit, clarifying the field of the IT audit, the methodology used, and how it is conducted. The first two sub-questions were chosen to provide a clear theoretical background with the third sub-question delving into the practical side of the research. The third sub-question was chosen to investigate the effects of an organizations migration to a cloud environment on the data integrity risks and how this influenced the IT audit method.

This research has adopted the action research methodology which is a cyclical process. This cyclical process consists of a theoretical and an empirical part. For the first step of the action research process, he previous chapters have built a strong informational background on the topics of cloud computing and IT audit through a thorough literature review.

Additionally, from the solid theoretical background on cloud computing and the IT audit, two expectations have been formulated. The two expectations have been clarified and formulated in section 3.2.4. An important part of the action research is diagnosis or analysis, namely of the current situation and how this is affected. The formulated expectations serve as ‘instruments’ for the analysis part of the action research cycle.

The next part of the action research cycle is empirical. An empirical base has been built on this informational background through a multiple case study as objects of research. According to Yin (2013), a multiple case study research would be the preferred method, as it produces more compelling evidence than a single case study.

Possible cases are identified and interview candidates have been considered. This research will perform interviews on two comparative case companies from the healthcare sector. The two chosen cases for this research are: Motion Health and Center Clinic; the former is using the ONS application on public cloud with SaaS, and the latter is internally hosting the application EPIC. In order to have a valid analysis, the two cases will be compared and cross analyzed. For the analysis part an ‘instrument’ is needed. In this research, the formulated expectations serve as ‘instruments’. The two case organizations will be described in detail in paragraph two.

The research method is qualitative, making it most appropriate whenever investigations are revolved around the daily routines of subjects (Mortelmans, 2009). Data has been collected through unstructured interviews with IT auditors in the exploratory phase, during the theoretical part of the action research cycle. In the evaluation phase, structured interviews are held with IT auditors in order to collect data.

Throughout the literature study unstructured interviews have been performed with the IT auditors. The data collected from these interviews in combination with the data collected from the literature review (see chapter two and three), has been used to formulate two questionnaires. The questionnaires have been used to collect data from the two cases, which will help us test the formulated expectations. The two questionnaires are similar in the questions asked, with the difference being: one questionnaire is focused on cloud computing and hence used in the case of Motion Health, while the second questionnaire is adapted for a traditional setting without cloud computing, used in the case of Center Clinic. The questionnaire for Motion Health can be found in appendix A and the questionnaire for Center Clinic can be found in appendix B.

The two questionnaires consist both of three parts: the first part which consists of the first two questions is focused on the structure of the client's organization and why the choice was made to outsource to cloud or respectively internally host their data and applications. Question three till six of the questionnaires focus on the role of the IT auditor and whether the IT audit has been affected and in what way. The third part of the questionnaires consists of question seven till ten and puts focus on the client's organization, how it has been affected and whether the relationship between the client and IT auditor has been affected. In both cases, the IT auditors got a bonus questions with regards to the future of cloud computing within the IT audit and what the IT auditor's predictions were for the future of their field.

Four structured interviews are held with different IT auditors of different management levels within EY for both cases, meaning two interviews for each case. Each IT auditor interviewee has been contacted through e-mail in order to introduce the researcher and topic of research. Subsequently, appointments have been made in order for the interviews to be held. The interviews were phone interviews, taking approximately two hours each. With the permission of the interviewees, the researcher has recorded the interviews and notes have been made. The recordings and notes have been further processed. Subsequently, the researcher has made sure that the processed notes have been send back to each interviewee by mail for a confirmation and to ensure their agreement with regards to the interview discussions. The interview protocol of this research can be found in appendix C.

For the last step of the action research method, the collected findings have been cross-analyzed and further elaborated upon. The findings from the interviews have fulfilled the empirical part of the research and have built upon the informational background. This has clarified how organizations have been affected by data integrity risks after they migrated to a cloud environment and how this subsequently affected the IT audit. From the collected data, the research has collected enough information to be able to provide an inclusive answer to the main research question. Additionally, the two formulated expectations are investigated with regards to the collected findings. The collected findings are further clarified in detail in chapter five.

Finally, in chapter six evaluations and conclusions are made, concluding the last step of the cycle. Subsequently, looking back at the performed research and explaining the limitations of the research and what kinds of future research can be performed to build on this study.

4.2 Case description

The two organizations are: Center Clinic and Motion Health. In order to prevent potential exposure of confidential information, the organizations' names are changed to fictive names. This research has specifically chosen healthcare organizations, since data integrity is crucial in healthcare. Organizations in healthcare work with confidential and very sensitive medical and personal information. Working with patients, it is important that patient records and information can be relied upon. Without the proper precautions, integrity constraints and implementation of effective controls, a small omission or error in data can have a big impact. It is important to have a reliable exchange of medical information and that medical errors are prevented. Having the right controls in place and maintaining data integrity is a crucial prerequisite.

Furthermore, the two organizations have similar applications that takes care of healthcare processes with regards to the process of medical information and communication between healthcare workers. The difference between the two organizations lies in their hosting of application and data. Motion Health has its application and data hosted on public cloud, with the SaaS service model (as was delimited in chapter two). Center Clinic on the other hand is internally hosting their application and data.

The difference between cloud and internally hosted, allows this research to outline the differences between their operations, safety measures and in what way data integrity is being maintained. Subsequently, this allows this research to compare findings from both organizations, allowing this research to draw conclusions that answer the main research question. Evidently, the only difference being cloud versus internally hosted, is another highlight that other possible effects and confounding factors have been controlled.

Five semi-structured interviews have been held with IT auditors during the literature study of this research. Additionally, a total of four IT auditors are interviewed with regards to this research. Two auditors have been interviewed on Motion Health and one auditor on Center

Clinic. An additional IT auditor is interviewed for healthcare organizations in general, which have outsourced to cloud using the same application as Motion Health and organizations that have internally hosted their applications and data. The fourth interviewee is specialized with clients in the healthcare sector, thus making him most suitable in providing this research with the necessary information with regards to cloud versus internally hosted in healthcare. Additionally, the fourth interviewee is in the best position to confirm the findings collected from the other interviews and providing the research with a distinct glance, having taken both sides into consideration.

Table 4 gives an overview of the interviewees participating in the research and organizations they are working on.

No.	Department	Name	Position	Case
1	Fait - ITRA	Marten de Bruin	Staff	Motion Health
2	Fait - ITRA	Bart de Jong	Senior Staff	Center Clinic
3	Fait - ITRA	Niek Blumer	Manager	Motion Health
4	Fait - ITRA	Erik Smeets	Manager	Healthcare sector

Table 4: the interviewees of two chosen research cases.

The content of the interviews is based on the literature overview performed during this research. The interview questions have been send in advance, giving the interviewees the chance to read through the questions before the actual interview. The interview questions for Motion Health can be found in appendix A and the questions for Center Clinic in appendix B. During the interview questions have been asked about the organizations' operations, what the effects are of the security risks on the organizations and data integrity, the effect it has on their IT audit activities and whether cloud has had an impact on their IT audit activities as a whole. In chapter five the collected data are cross-analyzed and clarified further. The two chosen cases Motion Health and Center Clinic are further clarified in detail below.

4.2.1 Case A: Motion Health

Motion health is a healthcare organization active in the fields of care, nursing and wellbeing for patients that require special care in the region of Eemland, the Netherlands. The organization was founded in 2007 and has grown since then with a turnover of €133.9M in 2014. At the moment Motion Health employs 2,500 employees and 2,000 volunteers working daily for their clients.

Motion Health has adopted the ONS application of Nedap. Nedap is an organization specialized in the development of applications and provision of solutions in the fields of security, automation and information management, having more than 80,000 healthcare organizations as clients. The Nedap ONS tool is a healthcare cloud application that gives care organizations the ability to optimize the different phases of the healthcare process from planning and scheduling to accessing medical records and communications between healthcare team members. ONS consists of the full client-patient administration of which all data are entered into the application panel and saved into the cloud at Nedap. Next to the client-patient administration, ONS can be considered an ERP for healthcare, taking care of all the billing, patient information and invoicing.

Two IT auditors are interviewed that work on the client Motion Health, as was shown in table 4. Interest is in to what security measures are in place and how the cloud security risks affect the organization. During the interviews the IT audit activities have been elaborated and data has been collected as to how the audit activities have been affected by the cloud application ONS.

4.2.2 Case B: Center Clinic

Center Clinic is a hospital opened in 1987 and originated from a merger of three regional hospitals. Center Clinic is a midsize hospital located in the Netherlands with around 1850 employees, 350 volunteers and 120 specialists. It offers a large array of healthcare services from all kinds of specialisms, with quality, involvement and personal care and attention being their most important characteristics.

Center Clinic works with the electronic health record (EHR) system EPIC. EPIC is internally hosted by Center Clinic and provides an integrated suite of healthcare services supporting the functioning of patient care (registration, scheduling), employee hours registration and billing and storing all data internally.

Similar to Motion Health, another IT auditor is interviewed that works on the client Center Clinic. The IT auditor has received similar questions as the IT auditors of Motion health. Interest is in to what security measures are in place and how the security risks affect the organization. During the interviews the IT audit activities have been elaborated and data has been collected as to how the audit activities are affected considering the security risks.

4.3 Research setting at EY

EY dates back to 1849 with the founding of Harding & Pullein in the United Kingdom. It took until 1989, before the current firm came to existence through a merger of Ernst & Whinney and Arthur Young & Co (EY, 2016a). Thenceforth, the firm was known as Ernst & Young until the first of July 2013, when Ernst & Young announced globally that it has adopted EY as its global brand name, unveiled a new logo and adopted "Building a better working world" as its purpose statement (EY, 2013).

EY is a multinational professional services firm and one of the "Big Four" audit firms. The firm is the most globally managed of the Big Four firms (consisting of Deloitte, PwC, EY, KPMG), sets global standards and oversees global policy and consistency of service, with the client work being performed by its member firms, which are run as separate legal entities in individual countries. EY has 212,000 employees in over 700 offices around the world and continues to make growth with a combined global revenue of US$28.7b for its financial year that ended 30 June 2015. Despite an uneven global recovery, and an economy with serious weaknesses and uncertainty, this was considered its highest revenue growth since 2008 (EY, 2015).

The global structure at EY is composed of the Executive, which includes global leadership and governance bodies, and Regions which are 28 regions grouped under four geographic areas: Americas, EMEIA (Europe, Middle East, India, Africa), Asia-Pacific and Japan (EY, 2016b). EY has four main service lines and share of revenues consisting of Assurance, Tax, Advisory and TAS (Transaction Advisory Services).

This research is performed within the IT Risk and Assurance department (ITRA). ITRA is part of the service line Advisory and is a specialized group within EY positioned at the intersection of Business and IT. ITRA is considered one of the major players in the market and performs IT audits focused on reliability, security and effectiveness of business information and control processes, with the IT audits taking place within the framework of the annual financial audit and beyond.

This chapter elaborated on the research process and clarified the subsequent activities and interviews to be held. Two chosen case companies have been selected and clarified and the interviewees have been selected. Subsequently, the research setting was explained. The four IT auditors have been interviewed and the collected findings are clarified and cross-analyzed in the next chapter.

5. Data collection and findings

The results of the interviews are discussed in this chapter. The chapter will commence with the effect of a migration to cloud on the clients' organizations in paragraph one. Secondly, the effects of a migration to cloud on the data integrity risks are discussed in paragraph two, followed by an elaboration with regards to the effects of a migration to cloud on the IT audit and the IT auditors' activities in paragraph three.

The discussions of this chapter are based on the findings, deducted from the answers of the different IT audit interviewees, supplemented with general findings collected from informal discussions with IT auditors from different management levels throughout EY. From the interviews and discussions it turned out that the IT auditors are quite unanimous in their answers.

5.1 The client's migration to cloud

The interviews all started with the question asking the interviewees to explain the structure of the organizations and what they considered as in scope and out of scope for their IT audits. In section 4.2 the organization's structure and their applications have been elaborated. Evidently, for the scoping it has become clear that Motion Health, which has outsourced to cloud, has also outsourced the maintenance and responsibilities regarding their application and data to the cloud provider. On the other hand, Center Clinic (internally hosting their application and data) has more responsibilities lying with themselves with regards to maintenance and control of application and data. This research was able to obtain an involvements table with regards to what is in scope and out of scope for both Motion Health and Center Clinic. However, considering confidential and company sensitive information, the involvements table of Center Clinic has not been included in this research. The involvements table of Motion Health can be found in appendix D. The involvements table of Center Clinic is similar to the one of Motion Health, with the only difference being that Motion Health has outsourced these responsibilities to the cloud provider while for Center Clinic these responsibilities lie with themselves. Which, confirms that the two cases are comparable.

As can be seen from appendix D, almost everything related to the ONS application has been outsourced to Nedap, except for the user and authorization management. Which is in line with the Clark & Wilson model. For the incident management it depends on the kinds of incidents. Incidents related to the application ONS is the responsibility of Nedap, while other incidents lie with Motion Health. For example, taking the risk ‘data leaks’, the incident can lie with Nedap or Motion Health, depending on what has caused it. Clarifying, a need for a procedure as part of incident management to determine this. It is clear that Motion Health has outsourced many of the responsibilities and processes to external parties, while maintaining only a few themselves. With the outsourcing, Motion Health needs to only maintain a few of the operations and processes themselves. This reduces the amounts of controls and procedures that could still be tested at the client. “Outsourcing to cloud has shrunk the scope. From now own only small parts can be checked and tested at the client” (M. de Bruin, interview, November 28, 2016). In addition to Service Level Agreements and monitoring of contract delivery, the parts that can still be audited and that are tested by the IT auditor at the client, are the parts for which Motion Health is responsible, see appendix D.

Comparing this with Center Clinic, which uses the internally hosted application EPIC, it becomes clear that Center Clinic has much more responsibilities. The responsibilities which have been outsourced by Motion Health, are still being handled and maintained by Center Clinic. From the interviews it has become clear that the IT auditor is testing much more at the client Center Clinic. Subsequently, leading to the IT auditors finding more points of attention with regards to unsecure procedures and controls, than is the case with Motion Health. “With the decision to internally host applications and data, Center Clinic has more responsibilities and needs to maintain much more than if they were to outsource to cloud. This has subsequently led to more work for us as IT auditors with regards to checking and testing controls and procedures at Center Clinic” (B. de Jong, interview, November 28, 2016). Relative to Motion Health, IT auditors have more work at Center Clinic.

The IT auditor is active in the annual audits, checking controls, applications and risks related to the annual audit. Eventually, this means that what is seen as in scope are all the applications, data and procedures which the accountant sees as relevant for the annual audit. “The auditor takes in to consideration and audits everything that the accountant sees as relevant for the annual audit. Applications and procedures not considered relevant, are not taken in to consideration during the audit” (B. de Jong, interview, November 28, 2016).

5.2 Migrating to cloud and the IT auditor

A question of interest for this research with regards to outsourcing to cloud, has to do with the consideration and choice of the organization to outsource and how this affects the IT auditor. From the interviews two very different views emerged with regards to why they opted for outsourcing or rather decided to locally host their applications and data.

Center Clinic opted for internally hosting the application EPIC and their data. Since, Center Clinic is a health organization with sensitive patient information which are confidential, they concluded that in order to protect this data against vulnerabilities and to make sure that the data is in the right hands, it was best for their organization to internally host their application and data. This is the sole reason Center Clinic is hosting their application and data in house, allowing them to take control of the data stream and all inputs and outputs with regards to the application EPIC.

It seems however, that majority of health organizations deviate from this way of thinking. “What we see is that majority of health organizations decide to outsource their IT applications and data to cloud for the following reason: they want to do the thing they are good at, namely providing healthcare. All other IT is considered a nuisance and can be outsourced” (N. Blumer, interview, November 28, 2016). Considering Motion Health, and this holds true for many other healthcare organizations that have opted for the ONS[10] application of Nedap; their choice for outsourcing has been made with regards to financial considerations and their own capabilities. Additionally, in their view an external provider can maintain security much better.

“Organizations often handle their own IT, whenever they make use of it extensively. However, when IT is not part of their core business and they can be considered end-users, then many organization make the choice of outsourcing to cloud” (E. Smeets, interview, November 29, 2016). Motion Health does not have a large IT department and they are not very devoted to IT. They do not see IT as a core part of their business and in order to put focus on their core business, namely providing healthcare services, they have chosen a cloud

[10] From the interviews it has become apparent that the ONS application from Nedap is quite popular among health organizations. Which means that the ONS application has been implemented for many health organizations (E. Smeets, interview, November 29, 2016).

provider with SaaS to outsource their needed applications and data. Looking at Motion Health, it becomes clear they do not have the capacity nor the quality in employment to maintain the applications and data. Having many applications with the combination of finding and employing the right people becomes unmanageable. Outsourcing to cloud makes them as an organization much more flexible and saving them financial costs[11]. From the interviews it has become clear that this is the way of thinking for majority of healthcare organizations that have opted for outsourcing to cloud. They outsource these responsibilities to the cloud provider, in this case Nedap. “After the outsourcing, it becomes Nedap’s responsibility to make sure that everything is running accordingly in the technical area and in the functional area making sure new updates, amendments and bug fixes are developed, published and implemented effectively” (E. Smeets, interview, November 29, 2016).

What does this mean for the IT auditors? Organizations are facing various risks. For these risks there are controls in place that need to mitigate or prevent these risks. The auditor is responsible for the testing of these controls. This is normally done at the client, but since the clients have outsourced their applications and data to the cloud, this is no longer possible. This would mean that the controls have to be tested at the cloud provider in order to provide assurance that the controls in place are effective for the parts of the outsourced application. However, this is also a burden on the cloud providers, in the case of Motion Health this puts a burden on Nedap. Nedap has many clients, and for all these clients audits need to be performed at the cloud provider in order to provide assurance that all controls are effective. “What Nedap does, is making sure that a thorough audit is performed and that all their controls are audited. Subsequently, they record this in an ISAE 3402 statement. With this statement, Nedap shows that their controls and procedures in place are operating effectively. Finally, this statement is delivered to the clients in order to give them assurance” (N. Blumer, interview, November 28, 2016).

The ISAE 3402 in this case is a SOC (Service Organization Control) 1 report (ISAE3402, 2016). SOC 1 reports on controls over processes that impact the financial statements. Additionally, there are two types of ISAE 3402 reports: type I and type II. Type I reports determine if all the mentioned controls of the ISAE 3402 exist and are adequately designed

[11] In house applications and data need to be secured, risks need to be mitigated and continuity needs to be ensured. This requires hiring the right personnel, time and effort, which all add to the financial costs for the organization in question, as there is a lot more to maintain and control.

for their objective. Adding to that, type II reports also determine whether the controls have been operating effectively for a full duration of a period. The type II reports provide the IT auditor with much more information for their assessment. Any further mentions of the ISAE 3402 report, refers to type II reports.

“What has changed for the IT auditor after a client’s migration to cloud, is that the IT audit activity has changed into the review and judgement of the ISAE statement, rather than the actual testing of controls at the client” (N. Blumer, interview, November 28, 2016). This is indeed in line with the second expectation, as formulated in section 3.2.4. Points of attention for the IT auditor has now become the checking of the ISAE 3402 statement, to make sure that the scope of the ISAE 3402 statement aligns with the scope of the annual audit.

There are many points for which Nedap bears the responsibility that they are tested and considered effective. On the other hand in the case of Motion Health, processes such as user and authorization management controls stay the responsibility of the client and Motion Health is also responsible that they are implemented effectively. In the case of Motion Health, the ISAE 3402 statement includes sufficient controls that check the database; i.e. which rights are assigned to the tables and what the authorization and administrative controls are. The only processes left to be tested at Motion Health, are generic healthcare processes, user management and password policy.

“The client outsourcing to cloud has limited the spectrum. With the use of SaaS, almost the entire process has been outsourced. The client does not have to do much. SaaS has pretty much taken over the audit. But, of course this depends on the degree of outsourcing. It is however the case, that from now on the IT auditor needs to ask for an ISAE 3402 statement, instead of personally testing the controls” (M. de Bruin, interview, November 28, 2016). Because of outsourcing to cloud, the IT audit activities have been limited to a certain degree.

A surprising discovery made from the interviews is that organizations in general do not properly consider the effects and changes before outsourcing to cloud. Next to this finding, it seems that organizations do not even properly discuss their requirements and expectations with the cloud providers. With regards to the agreements made between the clients and the cloud provider, it is clear that clients do not ask the right questions nor is there profundity in their conversations. “Whenever clients decide to outsource to cloud, they need to fully consider what they are outsourcing, what contracts and agreements are made with the cloud provider, whether the cloud provider can provide them periodically with an assurance statement (or that an IT auditor visits the cloud provider to perform an audit) and where the responsibilities lie of both the client and the cloud provider" (B, de Jong, interview, November 28, 2016).

This is in contrast to the first expectation, as formulated in section 3.2.4. This research expected clients to shift from an execution role to a direction role, with regards on what needs to be done. However it seems, that this is not the case. Instead, there is a lack of depth in the discussions with the cloud provider with regards to the controls in place at the cloud provider, the security measures, procedures, what happens in case of a calamity or change management. Additionally, This obscures the understanding of what the responsibilities are of the cloud provider.

What has been pointed out during the interviews is that most clients outsource their applications and data, further assuming that everything is handled correctly by the cloud provider. "Clients need to understand that they are not only outsourcing their data and applications, but also control. Eventually, what happens to the data will stay the responsibility of the client. Some clients tend to forget this. If a data leak happens at the cloud provider, it will be the client suffering from reputational damage, which subsequently could affect their financial performance. This is an important point, on which clients can improve and we do advise them take proper considerations and set up a package of requirements regarding the degree of assurance they need with regards to data, applications and procedures" (E. Smeets, interview, November 29, 2016). Most importantly, clients need to realize that eventually, whatever happens, they will stay the ones responsible for their data.

When it comes to the relationship between the IT auditor and the client, there is no significant change. What has changed is that the IT auditors are less present at the clients that have outsourced to cloud, since there are less controls to test at the client. The only controls that can still be tested at the client, are the ones which still lie under the responsibility of the client. This means that there is a shorter period to build a relationship between the client and the IT auditor. Subsequently, this means that the IT auditor has less contact with the client. However, the client stays the point of contact for the ISAE 3402 statement. With the absence of the ISAE 3402 statement; the IT auditor needs to perform tests at the cloud provider to still be able to provide reasonable assurance regarding the implementation of the right controls and whether they are operating effectively and maintained.

Another noticeable change in the relationship between the IT auditor and the client, is the type of conversations. “When the client has internally hosted applications, the conversations are more technical; what controls they have in place, how it is organized, what the procedures and policies are, how the infrastructure is organized (databases, operating systems) and further delving into the technical aspects of the controls. With the outsourcing, we now ask different questions: What controls the provider has in place, whether they are performing adequate tests, what agreements have been made, whether the cloud provider has it under control and how the client is monitoring this. We have different kinds of conversations with the client, when they have outsourced to cloud” (N. Blumer, interview, November 28, 2016).

In general with the clients outsourcing to cloud, there is a decrease in the IT auditor’s activities. The IT auditors have to do less themselves, since this is now done by the external party. It saves the IT auditor a lot of work, and additionally clients have to do less themselves. With the outsourcing, audits are processed much quicker now[12]. “A lot is done in advance with the provision of the ISAE 3402 statement, which provides the needed assurance. However, this also means that the IT auditor can give less recommendations now. “Having outsourced their application and data to cloud, it is harder to make recommendations as this is now under the full control of the cloud provider” (M. de Bruin, interview, November 28, 2016).

When asked what their predictions were for the future with regards to outsourcing to cloud and its effect on the IT audit, all interviewees were unanimous in their answer; it would lead to less work for the IT auditor in the context of annual audits, provided that the right controls have been put in place and depending on the degree of outsourcing. “Outsourcing to cloud leads to less work for the IT auditor, related to the outsourced applications. The work becomes more a review and judgement of the ISAE 3402 statement” (N. Blumer, interview, November 28, 2016). Additionally, all interviewees agreed that in the future more clients

[12] Although the audits are processed much quicker, since a lot is done in advance. The IT auditor still needs to check whether the scope of the ISAE 3402 statement is aligned with the scope of the annual audit. Additionally checking the period that is covered by the IT audit at the cloud provider in addition to checking the depth of tests performed. The IT auditor still needs to form a clear picture of the performed audits at the cloud provider on whether the right controls are emplaced.

would outsource their data and applications to public cloud.

5.3 The effect of cloud on data integrity risks

During the IT audits, the IT auditor tries to get an understanding of the SCOTs (see section 3.2), reviewing the IPEs (see section 3.2) to be able to conclude whether the accountant has correct and the right retrieval of information, and the actual testing of controls and procedures in place for the mitigation and prevention of risks. The interviewees were clear, that the IT auditor wants to know that security is ensured and that data integrity is maintained. With regards to the IPEs, as came out of the interviews, in general five risks are considered related to data integrity, accuracy and completeness:

1. Data processed by the application from which IPE is generated is not complete or accurate.
2. Data extracted from the application into the IPE is not the intended data or not complete. User parameters in IPE requests are not appropriate or incomplete.
3. There are inaccurate computations in the creation of the IPE from the application.
4. The data output from the application is modified or lost in the transfer.
5. New information added or changed is incomplete, inaccurate or inappropriate.

With these risks the IT auditor checks the input and output of data, the filters in place within applications, the performed queries and the databases.

It was noted however, that indeed these were the relevant risks tested by the IT auditor. But that the process of checking these risks had changed with the outsourcing to cloud. The data remains the responsibility of the client. From the outsourcing, IT auditors now check whether the cloud provider has effectively mitigated these risks according to the ISAE 3402 statement. “Eventually the auditor is responsible for the annual audit and needs to form a judgement on the controls in place. The auditor needs to know that the cloud provider has put these controls in place and that they are considered effective. Agreements need to be made between the cloud provider and the client to outline what controls are put in place and that they are effectively assessed. Then you also have agreements regarding bylaws, where the data is situated, uptime and downtime, what data is critical and which data has a higher priority in case of a calamity. For all this, the ISAE 3402 statement is suitable (including other TPM[13])" (B. de Jong, interview, November 28, 2016).

Clients which do not have outsourced to the cloud, required much more work from the IT auditor. In that case all controls in place are tested by the IT auditor at the client. In case of an outsourcing to cloud the IT auditor takes a look at what is included in the ISAE 3402 statement. Parts which do not lie under the responsibility of the cloud provider, still need to be audited and inspected by an IT auditor, the so called User Entity Controls. In the case of Motion Health, the client is still responsible for the user and authorization management. For the IT auditor this means that the access system to the ONS application is tested to see who has access to it, to review the user accounts and what authorizations are in place. Additionally, the accounts and password policy is investigated. As a result of the outsourcing, the database is maintained by Nedap; however, the access path and procedures of modifying and running queries (how they are set up and if they are secure enough) are still very relevant for the IT auditor. Of course the segregation of duties will be investigated, making sure the right people have access to the application and that there are correct profiles with standardized authorizations and rights. This, however is also partly the responsibility of the client.

With regards to the table of security risks (see section 2.3, table 3), a few risks came out as having a big impact on the data integrity, in the interviewees' respective views. "With a data breach, the hosted data can be edited either externally or internally and this endangers the accountability and justification. This makes the data unreliable as it influences the correctness and completeness of the data" (M. de Bruin, interview, November 28, 2016). All the interviewees agreed that next to data breaches, the risks: 'account or service hijacking', 'insecure interfaces and APIs' and malicious insiders could possibly have a big impact on data integrity. "Insecure interfaces and APIs can be very dangerous as this is responsible for the communication between applications. The data can be safe within the application, but during the transport, the data is vulnerable and attackers could abuse weaknesses if not secured properly" (M. de Bruin, interview, November 28, 2016). The same conclusions were made with regards to account or service hijacking. It was seen as a risk with a big effect on the data integrity, as the data could have been manipulated and therefore unreliable.

[13] A Third Party Memorandum (TPM) or third party declaration is a document issued by an independent auditing party about the quality of ICT services and - control of an organization. The TPM can include additional findings and measures of assurance that can support the audit of the client. Additionally, the TPM can be used to support the ISAE 3402.

Data leaks were not considered as a big risk on data integrity. "Data leaks are risks that lie with the cloud provider mostly and they need to make sure that sufficient backups are made. Additionally, agreements should be made with regards to what procedures are in place to prevent data leaks, and what will be done if it occurs. Data leaks do not really have an effect on data integrity and have a minimal effect on the internal data. It has a much bigger impact on the company's image, as they will suffer from reputational damage with regards to business continuity, if a data leak were to take place" (E. Smeets, interview, November 29, 2016).

During the interviews it became apparent that Nedap had previously suffered from a data leak in their servers. Motion Health was informed by Nedap, and it was disclosed that parts of their data was leaked from the servers at Nedap. As mentioned before, the clients always stay the ones responsible for their data. Motion Health could not do anything else than accept the fact that it had happened. It is then the responsibility of Motion Health, to disclose this information with their patients. Since 1st of January 2016, the law 'meldplicht datalekken' has been introduced in the Netherlands, forcing organizations to disclose sufficient information and publishing a statement whenever a data leak has occurred. With regards to the law 'meldplicht datalekken', the data leak was not significant enough in the case of Motion Health according to the interviewee, hence no public statement from Nedap.

This was a quite interesting finding. It seemed Nedap had failed in its promise of providing secure and reliable hosting of applications and data on the cloud. However, what is of interest is what this means for the clients; Do they take additional security measures, or perhaps sign additional agreements with the cloud provider? "The clients which have outsourced to cloud, do not have any additional security measures in place. Being healthcare clients, they do make sure that the cloud providers are certified with NEN 7510[14], and make agreements regarding that. Additionally, there is the ISAE 3402 statement. But, in reality, the clients do not really pay attention to these topics. They look at what is required (by law) and not required, when it comes to certain kinds of agreements and controls. Furthermore, they put their trust in the

[14] Healthcare organizations process and store important medical and patient data, which are considered sensitive and confidential. To ensure that all these data are securely stored, there is the NEN 7510 security standard which outlines, what the risks are and how they can be controlled.

cloud providers and assume that everything is reliable and under control" (N. Blumer, interview, November 28, 2016).

From the interviews it became clear that the current cloud security model is based on the assumption that the clients should trust the cloud provider. This was different for Center Clinic, which internally hosted their application and data. Center Clinic had many controls and procedures in place, NEN 7510 had been implemented extensively, there were checks and balances and were proactively performing attack and penetration tests to see what the vulnerabilities were, the impact they had and how they could be prevented. Subsequently, a phishing[15] awareness program was put in place, to have a clear understanding of how susceptible the employees were to phishing, how this could be detected on time and how to prevent it and educate their employees. Additionally, Center Clinic had a professional IT team, specialized in data security and attack prevention. Having a professional IT team, experienced with the IT systems in place at Center Clinic, the choice was clear to dismiss outsourcing to cloud.

For the Clark and Wilson model two aspects were of importance for ensuring data integrity, namely that data is only modified through well-formed transactions and that there is segregation of duty in place. Responsibilities regarding segregation of duty lies with both the client and the cloud provider. The client needs to ensure there is a secure account and password policy in place and that there is a clear understanding what authorization profiles exist and what rights they have. In addition, the cloud provider is responsible for ensuring that the right controls and safety measures are in place that enforce the segregation of duty in the process and the databases at the cloud provider. With regards to the well-formed transactions, it is the responsibility of the cloud provider that this is enforced. The two procedures in the Clark and Wilson model, namely the IVP (integrity verification procedures) and TP (transformation procedures) are performed in the cloud. The cloud provider needs to have controls in place that ensure the IVP and TP are correctly performed. In addition the right integrity constraints need to be in place that support these two procedures and enforce well-formed transactions. What integrity constraints are considered right, needs to be clearly discussed between the client and cloud provider.

[15] Phishing is when a malicious attacker is disguising as a trustworthy entity (i.e. employee) in an electronic communication, trying to obtain sensitive information such as usernames and passwords. Sometimes sending vulnerable links, to malicious contents such as spyware, viruses and malware.

With regards to change management, the cloud provider is at liberty to introduce any new changes, bug fixes and updates in the operating systems and applications. This happens occasionally and the clients are not always informed. Additionally, from the interviews it has become clear that clients do not really care about the changes made, as long as it is all ‘working fine’. Hence, not paying much attention to the changes and approving it, without realizing whether its affect their data in any way. Additionally, there seems to be a lack of monitoring of changes, on the client side. These adjustments made by the cloud provider could possibly impact the functionality of the systems which could lead to wrong data and improper transactions, thus increasing the uncertainty with regards to the transactions being well-formed.

From the interviews it has become clear that clients, outsourcing to cloud, have the idea that once they outsource their data and applications, they are also outsourcing all their responsibilities. This not the case; clients stay responsible for their data. Additionally, clients do not seem to ask the right questions to the cloud providers with regards to controls, procedures and other safety measures regarding their applications and data. It is assumed that everything is under control by the cloud provider. This does increase the uncertainty whether data integrity is actively maintained. Similarly, IT auditors review the ISAE 3402 statement and further assume that all controls have sufficiently been audited at the cloud provider. In particular, for systemic errors this is considered risky.

From the findings, it has become clear that only one expectations has come true. The findings were in contrast to the first expectation. Namely, this research expected clients to shift from an execution role to a direction role, with regards on what needs to be done. This was not the case. Instead, there is a lack of depth in the discussions between the client and cloud provider. Additionally, this obscured the understanding of what the responsibilities were of the cloud provider. The second expectation indeed came true. The IT auditor has indeed shifted from actual testing at the client to a more judgement and review of the ISAE 3402 statement.

This chapter provided a discussion regarding the findings of the interviews, comparing them to each other and highlighting the differences between outsourcing to cloud and internally hosting applications and data. The next chapter consists of a conclusion with a short discussion including the limitations of this research and further recommendations.

6. Conclusion and recommendations

This research was carried out to investigate the impact of a migration to a cloud computing environment on the data integrity risks and how this subsequently influences the IT audit. To be able to investigate this occurrence and provide an inclusive answer to the problem statement, discussed in chapter one, the following research question was formulated.

> What is the impact of an organization's migration to a cloud environment and how does it influence the IT audit method?

From this formulation, this research had commenced starting with a literature review, followed by interviews with candidates of interest and a discussion of the findings. This chapter will provide an answer to the research question, starting with the conclusion in paragraph one, recommendations in paragraph two and finally the limitations of this research in paragraph three.

6.1 Conclusion

In order to provide an answer to the main research question, two comparative healthcare cases were investigated, namely Motion Health and Center Clinic. The two healthcare organizations were similar in size, operations and in the applications used. The only difference between the two organizations was in their hosting of application and data. Motion Health has outsourced its application and data to a public cloud with the SaaS service model. On the other hand, Center Clinic is internally hosting their application and data. With the only difference being cloud versus internally hosted, other possible effects and confounding factors have been controlled. In total four IT auditors have been interviewed on both cases. Two auditors have been interviewed on Motion Health and one auditor on Center Clinic. Additionally, a fourth IT auditor specialized in health care organizations (both cloud and non-cloud) has been interviewed. The fourth interviewee was in the best position to confirm the findings and provided this research with a distinct glance, having taken both sided into consideration.

From the findings it has become apparent that clients migrate to a cloud computing environment for the benefits of cloud computing, namely less costs, less responsibility and allowing the clients to focus on their core business. However, in the eyes of the clients it seems that the benefits overpower the downsides of a migration to cloud. This is harming the correct assessment on whether they should migrate to cloud. This leads to clients putting their full trust and support behind the cloud provider, further assuming that from then on the cloud provider will have everything under control. Thus, overlooking the need for additional security measures, in particular with regards to integrity. Additionally, clients do not seem to realize that at the end it stays their own responsibility, whatever happens to the data hosted by the cloud provider.

The IT auditor used to perform audits locally at the client. This has changed now, with clients outsourcing their applications and data to external cloud providers. The IT auditor has now the possibility of a few different approaches. The IT auditor can perform audits at the externals cloud provider in order to assess their systems and controls. On the other hand, if that is not possible the IT auditor can judge and review the Third Party Memorandum (TPM) – ISAE 3402 statement. If it were the case that the cloud provider does not have a TPM or ISAE 3402 statement, then the IT auditor cannot deem the cloud provider's systems and controls as reliable. Then, the IT auditor could perform a substantive test to still assess the systems and controls.

When it comes to the auditing performed by the IT auditor, they look at the controls they expect and whether they are in place. What the IT processes are, whether they are performed correctly, what IT risks they could stumble upon and whether the right controls are in place to mitigate these risks. Afterwards they look at the TPM and ISAE 3402 statements, in order to check whether the right controls have been implemented that would prevent and mitigate the possible risks found. The TPM and ISAE 3402 statements are carefully evaluated and reviewed by the IT auditor to check whether it suffices and does not have any shortcomings. Finally, documenting all their findings in a special evaluation report.

With regards to the agreements made between the clients and the cloud provider, from the point of view of the IT auditors it is clear that clients do not ask the right questions nor is there profundity in their conversations. Clients themselves do not have insight in the risks they are vulnerable to, since they do not perform risk analyses. Additionally, they lack knowledge with regards to the necessary controls they need to mitigate the risks and whether the cloud provider has these controls implemented. Hence, a lack of depth in the discussions with regards to the controls in place at the cloud provider, the security measures, procedures, what happens in case of a calamity or change management.

This obscures the understanding of what the responsibilities are of the cloud provider and whether it has the right controls and procedures in place. Subsequently, causing uncertainty in whether data integrity is continuously being maintained, as it is hard to estimate whether the right controls and procedures are in place and maintained in case of a data integrity risk or whether an update or modification has hampered the upkeep of data integrity. To still have some assurance, a standard ISAE 3402 statement is signed, but this is not thoroughly discussed between the cloud provider and the client. Furthermore, it became apparent that the risks ‘data breaches, ‘account or service hijacking’ and ‘insecure interfaces and APIS’ had a big impact on the data integrity and that it was important for the client to take considerations with regards to these risks instead of blindly putting trust in the cloud provider.

The migration of a client to a cloud computing environment, is leading to less work for the IT auditor, with regards to the outsourced applications. With the migration, the IT auditors can perform less tests at the client, and alternatively are performing reviews and judgements on the ISAE 3402 statement to see whether the cloud provider has effective controls in place. However, it remained a question, whether the IT auditors were doing enough with regards to the reviewing of contracts and agreements between the clients and cloud providers. Subsequently, the relationship between the IT auditor and the client has been affected to a certain degree. The IT auditor is less present at the client, owing to the migration to cloud. This shorter relationship, subsequently means different conversations taking place between the client and IT auditor.

The migration to cloud means less can be tested at the client, which means less work for the IT auditor for the outsourced applications, since a lot has been done in advance, subsequently causing a change in the relationship between the IT auditor and client. Clients do not seem to properly discuss agreements regarding controls in place and alignment of responsibilities with the cloud provider, which does cause uncertainty in whether data integrity is being maintained. Instead clients assume that the cloud provider is in full control.

6.2 Recommendations

Throughout the findings it became clear that clients do not take the necessary effort to thoroughly discuss their prerequisites and agreements with the cloud provider, before migrating to cloud. Additionally, it remains the question whether the IT auditors are doing enough with regards to reviewing of contracts and agreements between the clients and cloud providers. Or even if they are proficient enough or have the proper knowledge to perform such activities.

It is recommended that before clients decide to outsource to cloud, that they internally discuss what their requirements are, what kind of controls they want and the degree of assurance they expect. Subsequently, it is best to lay out these prerequisites to the cloud provider and properly discuss: what controls the cloud provider has in place, what procedures are performed, whether they can provide assurance, ensuring that the responsibilities of both parties are clearly outlined and that data integrity will be maintained. Following proper considerations (e.g. risk management) will mitigate uncertainties with regards to data integrity and the safety measures in place and will place the client in a much safer position.

6.3 Limitations and future research

In this research several limitations can be acknowledged. The first limitation is the lack of case study interviews. For this research, two cases were chosen amounting to a total of four interviews with IT auditors of different management levels. Performing more interviews would provide the research with much more data on which the discussion and conclusions can build upon. The lack of interview was related to the second limitation, namely constraints on time and resources. This research had a time duration of six months, coincidently falling into the busy season of EY at the ITRA (FAIT) department, making it much harder with scheduling and finding the right amount of interviewees. Subsequently, limiting this research in gathering an exhaustive catalog of relevant evidence.

The interviews performed in this research were limited to IT auditors only. Clients and cloud providers were not interviewed in this research. On another note however, IT auditors perform a consultancy role, meaning they are best suited to provide this research with the client’s vision with regards to the questions asked. Thereby, making it possible for this research to include the client’s views indirectly through the IT auditors.

This research was limited to public cloud with the SaaS service model, additionally only researching two cases in the healthcare sector. This is another limiting factor, making it harder to generalize the findings to clients in other sectors with regards to the impact of an organization’s migration to a cloud environment and its subsequent effect on the IT audit method.

It will be quite interesting if additional research will lead to equivalent findings, when taking other sectors and other forms of cloud into consideration. Additional research is recommended to take a more thorough approach with performing more interviews and comparing the collected evidences from other forms of cloud in other sectors in addition to healthcare.

7. References

44 U.S.C., Section 3542. (2002). *Federal Information Security Management Act of 2002.* United States Code.

Al Saiyd, N. A., & Sail, N. (2013). Data integrity in cloud computing security. *Journal of Theoretical and Applied Information Technology*, 570-581.

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, 357-383.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., . . . Zaharia, M. (2010, April). A view of cloud computing. *Communications of the ACM, 53*(4), 50-58.

Arruda, L. (2015, October 26). *Cloud Services: IaaS, PaaS & SaaS - An infinity of acronyms*. Retrieved from Linkedin: https://www.linkedin.com/pulse/cloud-services-iaas-paas-saas-infinity-acronyms-leandro-arruda

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* (1st ed.). New York: McGraw-Hill Education.

Baskerville, R., & Pries-Heje, J. (1999, January). Grounded action research: a method for understanding IT in practice. *Accounting Management and Information Technologies, 9*(1), 1-23.

Big4. (2015, January 1). *THE 2014 BIG FOUR FIRMS PERFORMANCE ANALYSIS.* Retrieved from Big4: http://www.big4.com/wp-content/uploads/2015/01/The-2014-Big-Four-Firms-Performance-Analysis-Big4.com-Jan-2015.pdf

Blokdijk, J. (2004). Tests of Control in the Audit Risk Model: Effective? Efficient? *International Journal Of Auditing, 8*(2), 185-194.

Boritz, E. J. (2005). IS practitioners' views on core concepts of information integrity. *International Journal of Accounting Information Systems, 6*(4), 260-279.

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.

Chan, D. Y., & Vasarhelyi, M. A. (2011). Innovation and Practice of Continuous Auditing. *International Journal of Accounting Information Systems, 12*(2), 152-160.

Chou, D. C. (2015, June 20). Cloud computing risk and audit issues. *Computer Standards &*

Interfaces, pp. 137–142.

Christiaanse, R., & Hulstijn, J. (2011, March 27). *Neo-classical principles for information integrity* . Delft: Technology, Policy and Management.

Cisco Global Cloud Index. (2015). *Cisco Global Cloud Index: Forecast and methodology, 2014-2019.* San Jose: Cisco.

Clark, D. D., & Wilson, D. R. (1987). A comparison of commercial and military computer security policies. *IEEE Symposium on Security and Privacy*, 184-194.

Cloud Security Alliance. (2011). *Security guidance for critical areas of focus in cloud computing V3.0.* Seattle: Cloud Security Alliance.

Cloud Security Alliance. (2016). *The treacherous 12: cloud computing top threats in 2016.* Cloud Security Alliance.

Concrad, E., Misenar, S., & Feldman, J. (2010). *CISSP Study Guide.* Burlington: Syngress.

ENISA. (2009). *Cloud computing: Benefits, risks and recommendations for information security.* European Network and Information Security.

EY. (2013, July 1). *Ernst & Young rebrands globally*. Retrieved September 19, 2016, from EY - Global: http://www.ey.com/za/en/newsroom/news-releases/2013---press-release---july---ernst---young-rebrands-globally

EY. (2014). *Cyber insurance, security and data integrity.* EY.

EY. (2015, September 15). *EY reports 2015 global revenues up by 11.6%*. Retrieved September 19, 2016, from EY - Global: http://www.ey.com/gl/en/newsroom/news-releases/news-ey-reports-2015-global-revenues-up-eleven-point-six-percent#

EY. (2016a). *A timeline of our history*. Retrieved September 19, 2016, from EY - Global: http://www.ey.com/gl/en/about-us/our-people-and-culture/our-history/about-ey---key-facts-and-figures---history---timeline

EY. (2016b). *Our global approach*. Retrieved September 19, 2016, from EY - Global: http://www.ey.com/us/en/about-us/our-global-approach

EY. (2016c). *Audit [Company Learning Community Publication]*. Retrieved October 25, 2016, from EY Atlas: https://atlassearchlive.ey.net/#search/query=audit%20is?pref=20043/9/102

EY. (2016d). *USING GAM: Using EY GAM*. Retrieved October 26, 2016, from EY Atlas: https://atlassearchlive.ey.net/#document/421046/SL25378328-421046?pref=20043/9/102

EY. (2016e). *Assurance Services - Audit tools*. Retrieved October 26, 2016, from EY: http://www.ey.com/ch/en/services/assurance/financial-statement-audit/assurance-services_financial-statement-audit_-audit-tools

EY. (2016f). *EY IT processes: Glossary A-M*. Retrieved October 26, 2016, from EY Atlas: https://atlassearchlive.ey.net/#document/420861/SL25362675-420861?pref=20043/9/102&crumb=420968

EY. (2016g). *IPE: Information produced by the entity*. Retrieved October 27, 2016, from EY Atlas: https://atlassearchlive.ey.net/#document/421040/SL25377558-421040?pref=20043/9/102&crumb=420968

EY. (2016h). *SCOTS: Significant classes of transactions*. Retrieved October 27, 2016, from EY Atlas: http://atlassearchlive.ey.net/#document/421055/SL25379431-421055?pref=20043/9/102&crumb=8&query=scot

EY. (2016i). *CONTROLS: Controls over SCOTs and significant disclosure processes*. Retrieved November 1, 2016, from EY Atlas: https://atlassearchlive.ey.net/#document/420938/SL25376111-420938?pref=20043/9/102&crumb=8&query=manual%20control

EY. (2016j). *IT: IT processes*. Retrieved November 2, 2016, from EY Atlas: https://atlassearchlive.ey.net/#document/420968/SL25385035-420968?pref=20043/9/102

Grossman, R. L. (2009). The case for cloud computing. *IT professional*, 23-27.

Hansen, J. V., & Messier, W. F. (1982). Expert systems for decision support in EDP auditing. *International Journal of Computer and Information Sciences*, *11*(5), 357-379.

Harvard University. (2013, October 26). *Methods 4.* Retrieved November 23, 2016, from iSites Harvard University: http://isites.harvard.edu/fs/docs/icb.topic1344955.files/Methods%204.pdf

Hayes, B. (2008). Cloud computing. *Communications of the ACM, 51*(7), 9-11.

ISACA. (2011). *IT control objectives for cloud computing: controls and assurance in the cloud.* Rolling Meadows: ISACA.

ISACA. (2012, May 10). *Essential characteristics of Cloud Computing.* Retrieved from ISACA: http://www.isaca.org/groups/professional-english/cloud-computing/groupdocuments/essential%20characteristics%20of%20cloud%20computing.pdf

ISAE3402. (2016). *Service organization control (SOC) reports*. Retrieved December 26, 2016, from ISAE 3402: http://isae3402.com/ISAE3402_reports.html

Jaeger, P. T., Lin, J., & Grimes, J. M. (2008, December 12). Cloud computing and information policy: Computing in a policy cloud? *Journal of Informaion technology*

& politics, 5(3), 269-283.

Julisch, K., & Hall, M. (2010). Security and control in the cloud. *Information Security Journal: A Global Perspective, 19*(6), 299-309.

Kaliski, B. S., & Pauley, W. (2010). Toward Risk Assessment as a Service in Cloud Environments. *ACM HotCloud*, 1-7.

Knechel, R. W., & Salterio, S. E. (2016). *Auditing: Assurance and Risk* (4th ed.). New York: Routledge.

Lacity, M. C., Khan, S. A., & Willcocks, L. P. (2009). A review of the IT outsourcing literature: Insights for practice. *Journal of Strategic Information Systems*, 130-146.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing — The business perspective. *Decision Support Systems, 51*(1), 176-189.

Mayfield, T., Roskos, E. J., Welke, S. R., & Boone, J. M. (1991). *Integrity in automated information systems.* Alexandria: National Computer Security Center.

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology. *NIST Special Publication*, 800-145.

Mortelmans, D. (2009). *Handboek kwalitatieve onderzoeksmethoden.* Leuven: Acco.

Ramgovind, S., Eloff, M., & Smith, E. (2010). The Management of Security in Cloud Computing. *Information Security for South Africa (ISSA)*, 1-7.

Rathod, P., & Sapkal, S. (2014). Audit Service for Data Integrity in Cloud. *International Journal of Advanced Research in Computer Science and Software Engineering*, 288-292.

Sengupta, S., Kaulgud, V., & Sharma, V. (2011). Cloud Computing Security - Trends and Research Directions. *IEEE World Congress on Services*, 524-531.

Soxlaw. (2006). *Sarbanes-Oxley Act Section 404*. Retrieved October 25, 2016, from SARBANES-OXLEY ACT 2002: http://www.soxlaw.com/s404.htm

Statista. (2016). *Public cloud Infrastructure as a Service (IaaS) hardware and software spending from 2015 to 2026, by segment (in billion U.S. dollars).* Retrieved from Statista: https://www.statista.com/statistics/507952/worldwide-public-cloud-infrastructure-hardware-and-software-spending-by-segment/

Stewart, C., & Cash, W. (2005). *Interviewing: Principles and Practices.* Pennsylvania : McGraw-Hill Humanities/Social Sciences/Languages.

Tsidulko, J. (2015, August 1). *The 10 biggest cloud outages of 2015 (so far)*. Retrieved October 9, 2016, from CRN: http://www.crn.com/slide-shows/cloud/300077635/the-

10-biggest-cloud-outages-of-2015-so-far.htm/pgno/0/1

Tucker, G. H. (2001, September 1). IT and the Audit. *Journal of Accountancy, 192*(3), 41-43.

Van Praat, J., & Suerink, H. (2004). *Inleiding EDP-Auditing.* Ten Hagen Stam Uitgevers.

Wang, W.-T., & Chang, C.-F. (2016). *The adoption of cloud computing services: the moderating effect of organizational culture.* Hong Kong: PACIS.

Waring, J. J., & Bishop, S. (2003). “Water cooler” learning: Knowledge sharing at the clinical “backstage” and its contribution to patient safety. *Journal of Health Organization and Management*, 325 - 342.

Yin, R. K. (2013). *Case study research - design and methods.* Thousand Oaks: SAGE Publications.

Appendices

- Appendix A – Interview questionnaire Motion Health
- Appendix B – Interview questionnaire Center Clinic
- Appendix C – Interview protocol
- Appendix D – Involvements table Motion Health

Appendix A – Interview questionnaire Motion Health

Questionnaire (Motion Health – using the application ONS from Nedap):

1. Wat is de structuur van de organisatie en wat wordt er geaudit? Wat is in scope en wat is buiten scope?

2. Hoe heeft cloud computing (de keuze van) de klant beïnvloed? Wat is er veranderd? Wat wordt er anders gedaan?

3. Wat betekent cloud computing voor de IT auditor? Zijn er veranderingen in de IT audit activiteiten?

4. Zijn er specifieke aandachtspunten waar de IT auditor op moet letten, wanneer een klant gebruik maakt van cloud?

5. Houdt de IT auditor rekening met de data integriteit? Hoe wordt dit gedaan? (bv. IPEs, jaarrekening)

6. Welke risico's met betrekking tot data integriteit komen vaker naar voren bij de IT audits?

7. In **tabel 3** (paragraaf 2.3), vindt u een lijst met risico's. Welke risico heeft de grootste impact op de klant? Hoe zou dit de IT audits kunnen beïnvloeden? Zijn deze risico's voorgekomen bij de klant?

8. Wat betekent dit voor de IPEs en de SCOTs, kunnen ze als volledig betrouwbaar beschouwd worden?

9. Heeft de klant aanvullende beheersingsmaatregelen ingevoerd om deze risico's te beheersen?

10. Is er iets veranderd in uw relatie met de klant, aangezien ze nu gebruik maken van cloud? (bv. ISAE 3402)

11. In de zorg is de geheimhouding van patiëntgegevens van grootbelang, hoe houdt de klant hier rekening mee? Zijn er speciale afspraken of contracten tussen de klant en de cloud provider (NEN 7510)?

12. Wat is de toekomst van cloud binnen de IT audit? Wat voor effect zal het hebben op de IT audits? Betekent dit meer of minder werk voor de IT auditor?

Appendix B – Interview questionnaire Center Clinic

Questionnaire (Center Clinic – using the internally hosted application EPIC):

1. Wat is de structuur van de organisatie en wat wordt er geaudit? Wat is in scope en wat is buiten scope?

2. Waarom heeft de klant ervoor gekozen om alle data intern te hosten (EPIC)? Waarom geen cloud?

3,4. Stel je voor dat de klant gebruik zou maken van cloud? Waar zou rekening mee gehouden moeten worden? Verandert er iets in de IT audit activiteiten? Zijn er specifieke aandachtspunten waar de IT auditor op moet letten?

5. Houdt de IT auditor rekening met de data integriteit? Hoe wordt dit gedaan? (bv. IPEs, jaarrekening)

6. Welke risico's met betrekking tot data integriteit komen vaker naar voren bij de IT audits?

7. In **tabel 3** (paragraaf 2.3), vindt u een lijst met risico's. Welke risico heeft de grootste impact op de klant? Hoe zou dit de IT audits kunnen beïnvloeden? Zijn deze risico's voorgekomen bij de klant?

8. Wat betekent dit voor de IPEs en de SCOTs, kunnen ze als volledig betrouwbaar beschouwd worden?

9. Heeft de klant aanvullende beheersingsmaatregelen ingevoerd om deze risico's te beheersen?

10. Als de klant zou overstappen naar cloud, zou dit een impact hebben op de relatie tussen de klant en de IT auditor? Wat zou er veranderen?

11. Wat is de toekomst van cloud binnen de IT audit? Wat voor effect zal het hebben op de IT audits? Betekent dit meer of minder werk voor de IT auditor?

Appendix C – Interview protocol

This is the interview protocol of this research, with regards to the cases Motion Health and Center Clinic. The interview protocol below outlines the taken steps of the interview process.

Step 1:	Literature review on the topics of cloud computing and IT audit. Water cooler conversations with IT auditors with regards to possible cases and interviewees
Step 2:	Case selection (Motion Health and Center Clinic)

Step 3 (interviewee selection):

No.	Department	Name	Position	Case	Duration	Type
1	FAIT - ITRA	Marten de Bruin	Staff	Motion Health	2 hours	Phone interview
2	FAIT - ITRA	Bart de Jong	Senior Staff	Center Clinic	2 hours	Phone interview
3	FAIT - ITRA	Niek Blumer	Manager	Motion Health	2 hours	Phone interview
4	FAIT - ITRA	Erik Smeets	Manager	Healthcare sector	2 hours	Phone interview

Step 4:	The interviewees are contacted through mail to introduce the researcher and topic of research. Interview appointments are made.
Step 5:	Interviews are held. The interviews are recorded and notes are made by the interviewer.
Step 6:	The findings of the interviews and notes are further processed.
Step 7:	The processed findings and notes are send back to the interviews for a confirmation and to ensure their agreement with regards to the interview discussions.

Appendix D – Involvements table Motion Health

This is the involvements table of Motion Health clarifying the extent of external party's involvement with regards to the applications used by Motion Health. At the top, four applications can be found and at the left side the processes that are performed by either Motion Health or other external parties.

Applications → **Process(steps) ↓**	**Application 1**	**Application 2**	**Application 3**	**ONS Nedap**
Developing modifications	🟩	🟪	🟪	⬛
Testing modifications	🟫	🟫	🟫	⬛
Implementing modifications	🟪	🟪	🟪	⬛
Network and security	🟫	🟫	🟪	⬛
User and authorization management	🟫	🟫	🟫	🟫
Database management	🟪	🟪	🟪	⬛
Hosting and technical maintenance	🟧	🟧	🟪	⬛
Performing backups and restore tests	🟪	🟪	🟪	⬛
Incident management	🟦	🟦	🟦	🟦

🟫 = Motion Health	🟪 = Company A	🟧 = Company B
🟦 = Company C	🟩 = Company D	⬛ = Nedap