Linnæus University
Sweden

Degree Project at Master Level

Decision to migrate to the Cloud

A focus on security from the consumer perspective

Authors: Khaled Tawfique & Arlind Vejseli
Supervisor: Despina Fyntanoglou & Elissavet Kartaloglou
Examiner: Anita Mirijamdotter
Date: 2018-02-07
Course Code: 4IK50E, 15 credits
Subject: Informatics
Level: Masters
Department of Informatics

Abstract

Cloud computing is an emerging model in which applications, data, computing resources and operating platforms are provided to clients as a service. It represents a unique way to architect and remotely manage computing resources with minimal management effort or service provider interaction. As it become widely used and being relayed on, security and the risks surrounding it became more in focus to ensure the data protection. The purpose of the study is to focus on the security risks of confidentiality, integrity and availability, and how the cloud consumer perceives cloud security based on those risks. For this purpose, a qualitative research method was adopted and semi-structured interviews with 6 users with experience within the cloud were conducted to collect the data. The data were analysed and explained using codes and categories, based on the research questions and related literature. A roadmap was developed consist of four elements which can support in the migration decision. Those elements are: *Trust*, *Compliance*, *Proactive* and *Continuous assessment*.

Keywords

CIA, Security, Cloud consumer, Cloud migration, Trust, Compliance, Proactive, Continuous assessment

"If I have seen further than the others, it is by standing on the shoulders of Giants." Isaac Newton 1643-1727

Table of Contents

List of Tables and Figures

List of abbreviations

CIA:	Confidentiality, Integrity and Availability
CSA:	Cloud Security Alliance
IaaS:	Infrastructure as a Service
ISG:	Information Security Governance
NIST:	National Institute of Standards and Technology
PaaS:	Platform as a Service
SaaS:	Software as a Service
SLA:	Service Level Agreement

Chapter 1

1. Introduction

This chapter presents the background, problem statement, purpose, related studies regarding the research area are presented. Topic justification and scope and limitations among with the thesis organization for the research study are also presented.

1.1 Background and Problem Statement

Cloud computing is an emerging model in which applications, data, computing resources and operating platforms are provided to clients as a service (Malluhi and Khan, 2011). According to Oracle (2012, p. 4), cloud computing is highly important strategy for enterprises and ‘’*a combination of technologies and processes has led to a revolution in the way that computing is developed and delivered to end user’’.*

Cloud computing is a new terminology that was added to IT jargon in early 2007 (Hasan, 2011). It represents a unique way to architect and remotely manage computing resources with minimal management effort or service provider interaction (Hassan, James & Gail, 2010). Fang et al. (2011) define cloud computing as 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 (Barakovic and Husic-Barakovic, 2016).

There are basically five stakeholders or actors playing the main role in the cloud migration and maintenance. The NIST cloud computing reference architecture defines those major actors (Figure 1.1):

- Cloud consumer
- Cloud provider
- Cloud auditor
- Cloud broker
- Cloud carrier

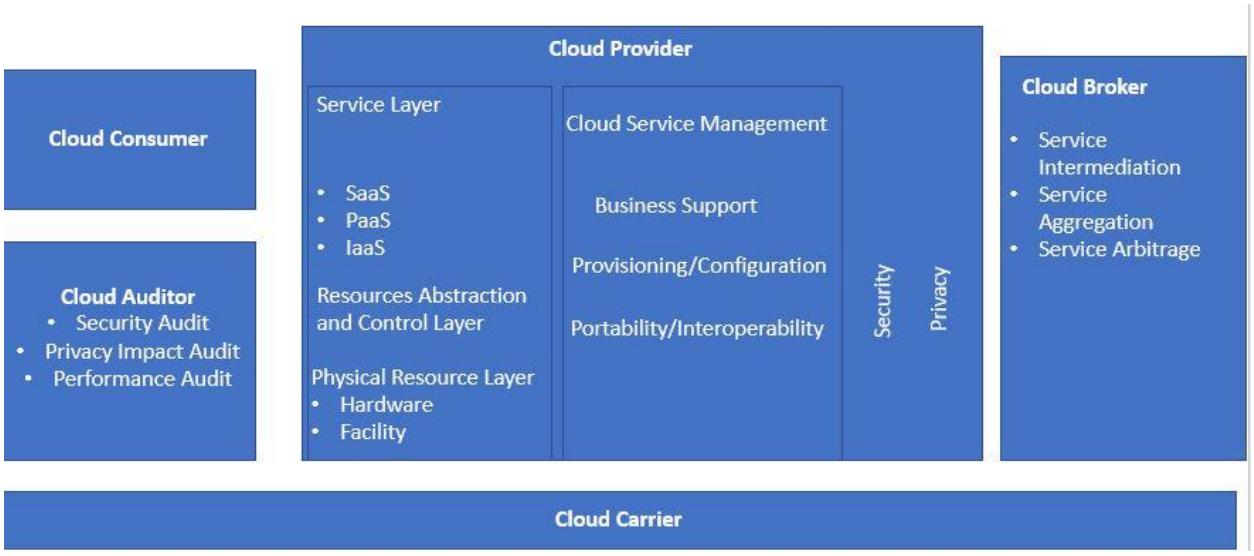

Figure 1.1: The Cloud Computing Conceptual Reference Model (Fang et al., 2011)

Each actor is an entity (a person or an organization) that participates in a transaction or process and/or performs tasks in cloud computing (Fang et al., 2011).

The *cloud consumer* is the principal stakeholder for the cloud computing service. A *cloud consumer* represents a person or organization that maintains a business relationship with and uses the service from a *cloud provider*. On the other hand, the *cloud providers* are responsible for making the service available to *cloud consumers*. The *cloud brokers* manage the use, performance, and delivery of cloud services, and negotiate relationships between *cloud providers* and *cloud consumers* (Fang et al., 2011).

The *cloud auditor* is a party that can conduct independent assessment of cloud services, information system operations, performance, and security of a cloud implementation. A *cloud auditor* can evaluate the services provided by a *cloud provider,* in terms of security controls, privacy impact, performance, etc. In most cases, the *cloud auditor* is conducting the assessment based on the request from the *cloud consumer*. Finally, the *cloud carrier* is the intermediary that provides connectivity and transport of cloud services from *cloud providers* to *cloud consumers* (Fang et al., 2011).

Sid Nag, research director at Gartner, Inc., highlighted in 2016 Cloud market growth annual report: "*This strong growth continues reflect a shift away from legacy IT services to cloud-based services, due to increased trend of organizations pursuing a digital business strategy*" (Gartner, 2016). The cloud computing paradigm enhances collaboration, agility, scalability, and availability for end-users and enterprises. It provides optimized and efficient computing platform, and reduces hardware and software investment cost, as well as carbon footprint (Bojanova, 2011). For example, looking on the business Spotify, the leading music streaming company, has been leasing and buying its own data centers to provide its streaming services. In 2016, the company decided to move into Google Cloud Services. The early focus on hosting an on premises was "*operating our own data-centers may be a pain, but the core cloud services were not at a level of quality, performance and cost that would make cloud a significantly better option for Spotify overall*," however by the time, Spotify recognized that ‘’*storing data on the cloud was high enough quality not to merit the extra cost and scaling issues of spinning up their own servers’’* (Konrad, 2016). This encouraged the company to move towards the cloud computing services. This shows even though the *‘’IT infrastructure is shifting from locally managed software enabled platforms and physical hardware to outsource virtual infrastructure’’* the adoption is going slower than expected (Ismail, Islam, and Mouratidis, 2015, p. 1).

As the cloud services, have increased by 19.5% in 2016 comparing to 2015, it has been noticed a significant increase in cloud management and security services by 43% (Gartner, 2017). The security services are forecasted to grow by more than 200% by the end of the decade (Gartner, 2017). Security attracted more attention of IT managers than ever before, and as the threats and vulnerabilities become more complex. The solutions and systems for responding to those threats are becoming more agile and integrated into the overall picture, of what it means to work in the cloud (Prendergast, 2016). As Kalloniatis et al. (2014, p. 1) stated, *‘’one of the major research challenges for the successful deployment of cloud services is a clear understanding of security and privacy issues on a cloud environment’’*.

The decision to migrate to the cloud can be defined within the migration framework. The decision components divide into three aspects as shown in figure 1.2:

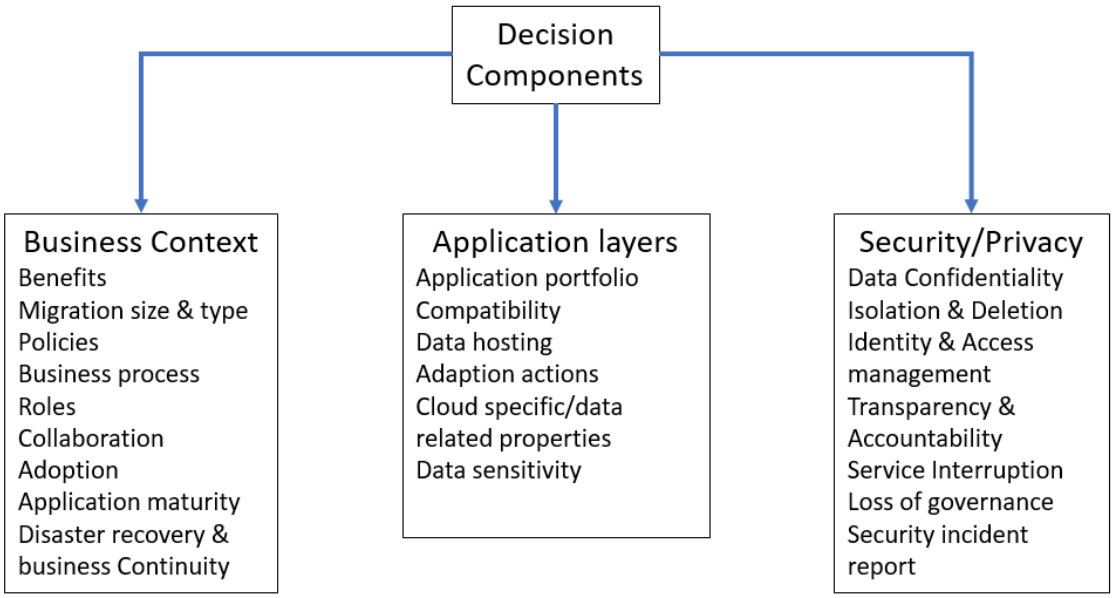

Figure 1.2: Decision Components (Islam, Weippl, and Krombholz, 2014)

Business context considers the issues based on the business and organizational needs, for example, organization entities, IT usage, costs and benefits of migration. On the other hand, *application layers* are to understand the characteristics of the application without using any cloud technology. This process and analyses allows to identify which part of the application or maybe all should be migrated to the cloud. Finally, the *security/privacy* aspect such as attacks against cloud infrastructure, unauthorized access, or DoS are among major challenges that can prevent and delay the organization's decision to migrate. (Islam, Weippl, and Krombholz, 2014). Thao and Omote (2016) stated that the rapid growth in the cloud services also introduces new security challenges, which require an extra effort such as data auditing to ensure data *availability*, *confidentiality* and data *integrity* in the cloud. Therefore, it is important to clarify the concept of the *CIA triad*. *CIA* stands for *confidentiality,* integrity and *availability*. Per the NIST Glossary of key Information Security terms, *confidentiality* is *''preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information''*, *integrity* defines as *''guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity''* and finally *availability* is *''ensuring timely and reliable access to and use of information''*(Kissel, 2013, p. 17; p. 45; p 101).

Researchers have argued about identifying the risk factors in cloud security. Islam (2014) identified *12 risk factors*, such as *data confidentiality*, *identify* and *access management*, *services interruption*, associated with the cloud migration so that appropriate control measures can be taken. However, the *Cloud Security Alliance* (CSA) mentioned in their textbook for Best Practices Mitigating Risks only *11 risk factors* which can impact one of the CIA triad (Kapil and Kelvin, 2015). A research made by Chandran and Angepat (2010) claims that *integrity* affects the accuracy of information in the system. *Availability* is an important part in cloud computing since the need of the customers should be fulfilled in time. *Confidentiality* is also an issue that is associated with

cloud computing. Disclosing information to cloud providers could lead to consequences such leaking data or information which can have a negative impact on their business.

Therefore, in this research paper we will focus on the security/privacy aspect as it is important to identify potential risks and prevent those risks that can occur during the migration, which can affect the organization's current work situation.

Thus, in our research, we have chosen to focus on how the cloud consumer perceive cloud security based on the risk factors confidentiality, integrity and availability, during the migration process. This can generate value for organizations that wants to migrate to the cloud, since they can avoid problems in an early stage of the migration (Thao and Omote, 2016).

1.2 Related Studies

Yigitbasiogly (2015) examine external auditors and why organizations do or don't adopt cloud computing. The study was qualitative where interviews were conducted with accountants and IT personal. The interview questions were based on risks, adoption, acceptance, and motives of cloud computing. Large accounting firms where auditors were working using public and private cloud services. The result of the research shows that data confidentiality and involvement of foreign authority remain as a concern, especially if the data is outside Australia. To minimize the risks with cloud computing, organizations have started to use hybrid solutions or private clouds that have national or dedicated data centers. The research is also the first empirical study that reports cloud adoption from the cloud auditors' perspectives.

Prasad, Green and Heales (2014) performed a study that is suggesting IT governance structures to manage the cloud computing services. Cloud computing services presents how organizations should manage their IT expenditure and access to modern IT resources. To manage the cloud computing services, organizations need to have governance structures and policies. This will generate to an effective management of the cloud computing services. A quantitative study was conducted with 126 respondents, where 26 respondents were actual adopters and 110 respondents were potential adopter of cloud computing services. The result of the survey data suggests that governance structures would contribute immediately to cloud computing that is related to business objectives. It will also contribute to financial objectives indirectly that is within cloud computing.

Chandran and Angepat (2010) analyzed three risks associated with cloud computing – security risks, privacy risks and consumer risks. The study was conducted by examining several terms of services and policies regarding copyright and privacy. By exploring the risks within these documents, two questions arose – *"how to estimate data security risk before placing data in the cloud and how to assure customers that their data is safe with the service various providers within the cloud network?"* The result of the study showed that there is a lack of risk analysis in the cloud computing environments. Risk analysis approaches needs to be performed to help customers and service providers. The study also showed measures such as trust and confidentiality that could be taken when using cloud computing to minimize negative effects.

Tchernykh et al. (2016) examine in their article the user's perception of the intentions and actions of cloud providers. The two main topics in the article is how to provide reliability, safety and privacy of information, and how to deliver powerful cloud behavior under specific constraints in attendance of the risks of confidentiality, integrity and availability. The aim of the paper was to find solutions that performs well to different insecurities. Sources of insecurity and basic

approaches for scheduling insecurity are reviewed before the research to get an understanding of the area. They also reviewed sources of uncertainty and basic approaches for scheduling during uncertainty to get data. The results of the paper present the understanding of how to model cloud computing with uncertainty resource provisioning in different cloud environment such as, *hybrid private-public cloud environment, dynamic self-adaptive distributed brokering, elastic clouds,* and *optimization of related problems to deliver powerful resource management solutions*.

Theoharidou et al. (2013) paper examines privacy risk assessment for the cloud and identifies different threats like vulnerabilities and countermeasure. The migration of data and applications to the cloud shows new threats and vulnerabilities. Authorities and auditors needs to hold providers accountable for their action. Theoharidou et al. (2013) examined how privacy risks are introduced when data and applications are migrating to the cloud.

Previous studies in the cloud services area concern various aspects, including discussion about cloud services in a general perspective and what benefits and disadvantages it can generate for an organization before and after migration. It also concerns how the stakeholder's intentions can affect an organization associated with migration to the cloud, such as changing working routines, new processes and guidelines, but also risks that may arise. Therefore, it is important to eliminate early-stage risks to more easily meet successful migration.

Since cloud services are a wide area of information technology, it is important to understand the cloud services, so that you can form a general view before specifying it to a level of detail. To eliminate early-stage risks and based on previous studies we will focus on one stakeholder, the consumer, and how this stakeholder perceives cloud security based on the security risks of confidentiality, integrity and availability in the migration process. The selection of the consumer as they are the end users and the principal quality driver and constraining influence as well the most impacted in case the migration failed Vouk (2008). The result of the study should then be used as a basis for future organizations, regardless of size, which plans to migrate to the cloud. This can eliminate potential risks that can occur and facilitates the work with the migration.

1.3 Purpose Statement and Research Questions

Based on previous studies in the cloud area, research has been conducted at a general level, where several aspects of the cloud environment have been investigated and what it can generate for benefits and disadvantages. The inability of a cloud stakeholder can have a negative impact on the organization associated with a cloud migration, such as security risks and changed routines and processes. Eliminating early-stage risks assist the organization to achieve a successful migration with minimal risks. Since the cloud migration area is a broad topic, we selected to focus on the security of cloud migration from the consumer perspective to explore. Therefore, the study intends to find out the focus on the security risks of confidentiality, integrity and availability and how the cloud consumer perceives cloud security based on those risks.

To fulfil our purpose of the research, two questions will be answered:

- How the consumers perceive the cloud security in terms of confidentiality, integrity and availability, in the migration process?

- Which elements to consider for a successful migration from security perspective?

1.4 Topic Justification

Cloud computing is a new IT service as it represents a unique way to architect and remotely manage computing resources, with minimal management effort or service provider interaction (Hassan, James and Gail, 2010). However, the use of the cloud can be a security threat, because confidential data that is stored in the cloud can be accessed if the security is low or unsecure (Singh, Jeong and Park, 2016). This research can be used by private individuals and organizations that choose to migrate and store information and data in the cloud. For this reason, it is a critical area to investigate in, since the data security is a topic that concerns every user. For example, Cloudbleed incident that took place earlier 2017, a bug was discovered by Google security researchers, which allowed them to access what was supposed to be private web data supported by Cloudflare (Wolff, 2017).

Studies within this research shows e.g. why organizations do or don't adopt cloud computing and user's perception of the intentions and actions of cloud providers. Cloud services can be extremely beneficial, since it has become a defining IT technology where organizations can move its resources (Posey, 2013). We have therefore chosen to focus on the security risks from the perspective of the cloud consumer based on *confidentiality, integrity,* and *availability* (CIA) during the migration process; and to construct a roadmap to provide the consumer with basic understand for the elements surrounding the security plan.

The result of this thesis will allow organizations planning to migrate to the cloud to build a framework enhancing a successful migration to the cloud. This will lead to minimal risks and avoid failure to migrate, since the results will be used to prevent a failure and reduce risks. We have selected personnel who worked during the migration process to the cloud to get their experience and lessons learned from the gained knowledge in cloud security.

1.5 Scope and Limitations

The scope of the study is to investigate the risks and elements that can emerge during the migration process; And organize the elements around the security plan to allow the consumer to identify them in initial stages to prevent failure and enhance the success of the migration process.

The research will be conducted with participants that have already worked on migration projects and have work experience within the cloud.

The limitation of our study is to investigate the security risks from the perspective of the cloud consumer based on, confidentiality, integrity and availability during the migration process. Perceptions of other cloud stakeholders will not be explored in this research study. The motivation of the delimitation for this research was selected to target medium-large organizations from different industries that already migrated to the cloud, due to business contacts and to obtain those organizations experiences.

1.6 Thesis Organization

The thesis will be divided in six different section and will begin with an introduction and end with a conclusion, as *figure 1.3* shows.

Chapter 2 – Literature review
This section will present the theory regarding cloud computing and previous studies related to the research area.

Chapter 3 - Methodology
In this section, the methodological approach, methodological tradition, data collection method, data analysis and the ethical consideration will be presented.

Chapter 4 – Empirical findings
This chapter will describe the empiricism from the data collection.

Chapter 5 – Discussion
The empirical findings will be discussed and analyzed in this chapter.

Chapter 6 - Conclusion
In this section, a summary of the findings and analysis will be described. Future research will also be described in this section.

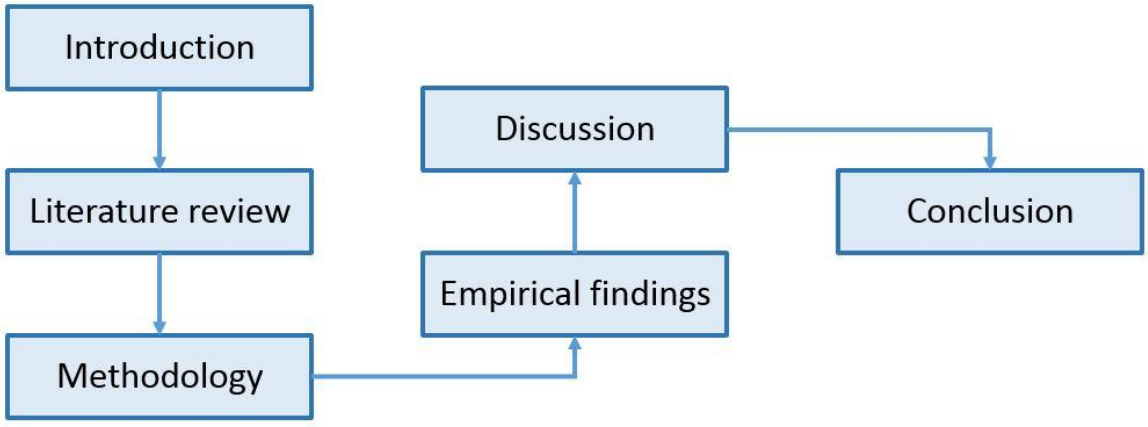

Figure 1.3: Mapping the research structure

Chapter 2

2. Literature review

This chapter will present relevant theory within the research area. Theory regarding cloud computing, cloud computing service models, cloud computing deployment models and cloud security. The chapter will end with the theory of the CIA and the information security concerns.

2.1 Cloud computing

Cloud computing is a service that can be described as a set of computing resources, which can be used with the lowest effort and lowest provider interaction. It is also indicated by broad network access, resource pooling, and on-demand self-service (Mell and Grance, 2011). Buyya, Broberg and Goscinski (2011) claims that cloud computing is based on four areas of technology:

- Internet technologies
- Hardware
- Distributed computing
- Systems management

Information and communications technology (ICT) has led to important improvements within these four areas, which leads to the development of cloud computing. The Internet technologies accepts different applications on servers and computer to transfer and exchange data. To collect the organization's data from multiple servers, it is important that technologies of distributed computing is critical since it allows for accessibility (Buyya et al., 2011).
The hardware has an important role for instance hardware virtualization, because it allows users to share the same resource in the servers. For example, one server can host one organization's data and operations. Cloud services are also backed up by physical servers, that are collected in data centers which includes thousands of computers (Buyya et al., 2011).

2.2 Cloud computing service models

According to Ramgovind, Eloff and Smith (2010), the next security consideration is to consider the sort of cloud computing service models, which organization management needs to do. The architecture of cloud computing can be categorized into three types – *Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).* The three cloud computing service models and its responsibilities are shown in *figure 2.1*.

- *Software as a Service (Saas)* – This model allows the capability to use the applications on a cloud infrastructure. The customer does not need to buy software, since they are leased out to contracted organization. It is either a pay-per-use model or for free limited use. The applications are accessed by using a web browser through the Internet or by using a program. The customer does not control or maintain operating systems, network and other application capabilities. This is the underlying infrastructure of the cloud (Ramgovind et al., 2010).

- *Infrastructure as a Service (IaaS)* – The IaaS model dedicates its resources to contracted clients and organizations that are at a pay-per-use fee. This means that investment must be

made in computing hardware such as processing powers, servers and networking devices. It allows degrees of financial and functional flexibility that are not found in internal data centers. This means that computing resources can also be quickly and cost-effectively than in a data center. Applications based on IaaS are mostly delivered through the Internet to the firewall that the organization is using (Ramgovind et al., 2010).

- *Platform as a Service (PaaS*) - This model works more like the IaaS but provides another functionality, which can be perceived as a rented functionality. Customers can transfer more costs from the capital investment to operational expenses. Virtual machines must be protected in the PaaS layer, because malicious attack like cloud malware is occurring. It is important to maintain the integrity of application during the transfer of data (Ramgovind et al.,2010).

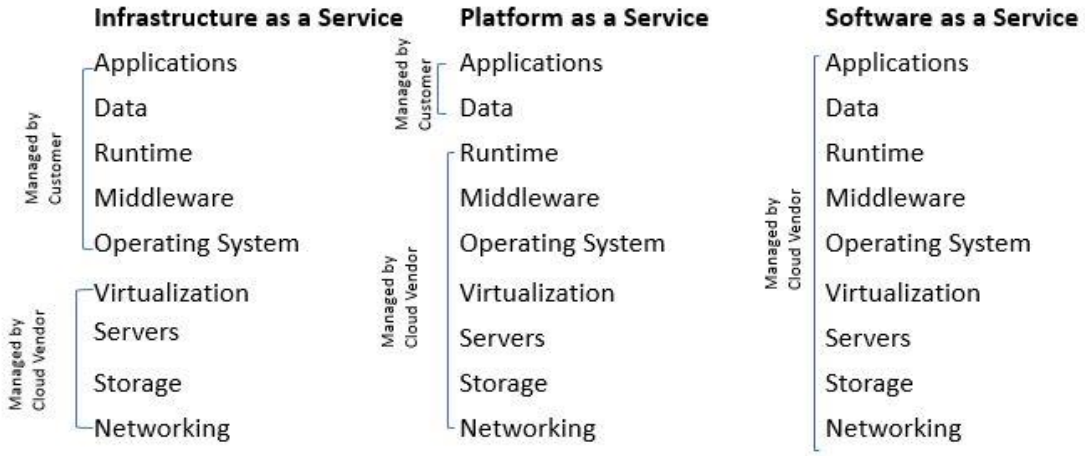

Figure 2.1: Cloud responsibilities (Kilström, 2016)

2.3 Cloud computing deployment models

Carroll (2011) describes that cloud computing services and technology are deployed over different types of delivery models based on the characteristics and purpose. The deployment scenarios include:

- *Public cloud*
- *Private cloud*
- *Hybrid cloud*
- *Community cloud*
- *Virtual private cloud*

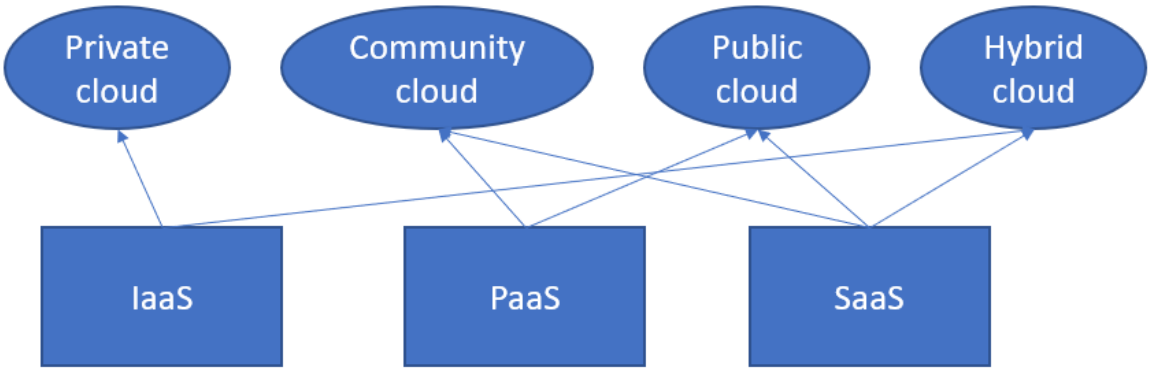

Figure 2.2: Relation of the deployment models and the platform (Shields, 2014)

• *Public cloud* – The infrastructure of the cloud is available to industry groups and is owned by organization's selling cloud services (Fang et al., 2011).

• *Private cloud* - The cloud infrastructure is operated for an organization that can be managed by the organization or an external actor (Fang et al., 2011). In this model, the cloud computing provider owns the data center and maintain it. The advantage is to make it easier to manage security, upgrades and system maintenances, which provides more control over the deployment and the use of it. Compared to the public cloud, where service provides the applications and resources, these are unified together and available for the users at the organization level in the private cloud. The organization are managing the resources and applications (Jadeja and Modi, 2012).

• *Community cloud* - The cloud infrastructure is divided by various organizations and supports a specific community that has shared matters, for example missions, policies and security requirements. It may be managed by the organizations or an external actor and can exist on-premise or off-premise (Fang et al., 2011).

• *Hybrid cloud* - The cloud infrastructure is a structure of two or more clouds, for example private, community, or public clouds, that remain unique units, but are bound together by standardized or own technology that enables data and application portability (Liu, 2011).

2.4 Cloud security

Cloud security is a part of computer security and describes a collection of technology, control and policies that is useful for the data protection and it services. Threats and attacks affects the cloud system whether it is directly or indirectly (Ashish and Kakali, 2017).

Ashish and Kakali (2017) describes that the cloud security covers several security issues and threats like:

- Virtualization
- Multi-tenancy

- Cloud platforms
- Data outsourcing
- Data storage standardization
- Trust management

Virtualization is a process that is extracting operating systems, services and applications from the hardware on which they run. The Virtual Machine (VMs) and Virtual Machine Manager (VMMs) are included in the virtualization and are related as a component (Ashish and Kakali, 2017).

Multi-tenancy is a feature of the cloud that allows the users to access the resources in a common way. This feature is a major part of the cloud that leads several security issues (Ashish and Kakali, 2017).

Cloud platforms allows users to lead their applications and services to the cloud, for example Virtual Machine Manager (VMM) is a cloud platform for IaaS services, .NET and Java Virtual Machine (JVM) is used as a development platform by the users (Ashish and Kakali, 2017).

Data outsourcing is used by organizations for their business purpose. It means that people gives data collection to a third-party provider and provides both operational and capital investments (Ashish and Kakali, 2017).

Data storage standardization gives organizations high level certification to their customers based on the authority like International Organization for Standardization (ISO). Data processing is a difficult task in the cloud since the cloud holds big amount of data. Therefore, a backing policy is required for the organizations (Ashish and Kakali, 2017).

Trust management is a parameter in cloud security that cannot be measured. It is based on the decisions regarding the data center, the hardware, the network configuration and the self-infrastructure. The trust issues occur in the cloud, due to customer data that are managed by second or third party (Ashish and Kakali, 2017).

Zanella (2010) states that when an organization is moving to the cloud, the important thing to know is whether their data will be secured and protected from being accessed by unauthorized individuals, as well ensure that the regulations and mandates for the security is updated and complaint. A survey conducted by Zanella in 2010 on 159 enterprises that was planning or moving to the cloud. In the result of the survey, security concerns and risks were founded regarding this area according to Zanella (2010). These were:

- Requirements of control or visibility over processes
- Requirements of security and privacy guarantees
- The costs of compliance and security
- Movement and control of data location

An analyze of the study claims that these concerns and risks of the cloud security can be summarized as *control* and *confidence.* IT and business managers have less *control* over its resources and information in a cloud environment. The *confidence* for the managers will be less that they will stay secure and collected. In today's IT environments, most of the IT managers have

control over its resources and information since they know their location and there is also a certain ownership (Zanella, 2010).

2.4.1 Perspectives on cloud security

Zanella (2010) states that there are three different use cases to observe regarding cloud security – security *for* the cloud, enterprise security *to* the cloud and security *from* the cloud. The three use cases are showed in *figure 2.3*.

Enterprise security to the cloud

The organization has its own security adapted for each business section, for example provisioning. If the organization wants to extend the existing security, they must use the services that are accessible through the cloud. This is showed as number *"1"* in figure 2.3 and the line shows the flow of the information or the service. This type of alternative would generate an automated provisioning to cloud applications like Google Apps or Amazon. The security software is running in the client IT environment that communicates through standards-based interfaces in the cloud (Zanella, 2010).

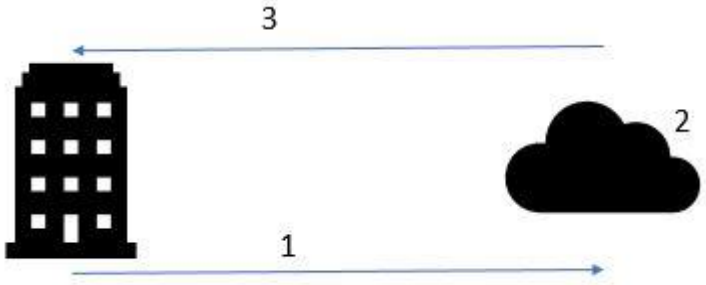

Figure 2.3: Security to, for and from the cloud (Zanella, 2010)

Security for the cloud

In this case, security controls need to be created by the cloud provider to protect data and applications in the cloud. There is a security software in the cloud that protects the servers and information that are stored there. This information does not have to belong to the cloud provider since it can belong to the customers of the provider. To fulfill the security requirements, the cloud provider needs to duplicate the controls that are in the local environment or create a new. For example, aspects like access management, data and access control would be included (Zanella, 2010).

Security from the cloud

The cloud provider is supposing security services to a client's IT organization. These means that the client does not need to create and maintain security services in their environment. Important data will still belong to the client. This aspect is an effective method to control various security and privacy issues (Zanella, 2010).

2.5 Information security concerns and challenges (CIA)

Building new services in the cloud or even adopting cloud computing into existing business context in general, is a complex decision involving many factors. Enterprises and organizations must make their choices related to services and deployment models, as well as, to adjust their operational procedures into a cloud-oriented scheme combined with a comprehensive risk assessment practice resulting from their needs (Kalloniatis et al., 2014).

Managing the cloud infrastructure is a challenging task. Reliability, security, quality of service, performance stability, and cost-efficiency are important issues in these systems (Tchernykh et al., 2016). Security and privacy issues are among the most important concerns that primarily hinder the migration decision. A recent survey of potential cloud adopters indicates that security is the primary concern hindering its adoption (Islam, Weippl, and Krombholz, 2014).

''Information security assumes defending information from unauthorized access, use, disclosure, disruption, modification. It is important to design a secure and fault tolerant multi-cloud environment, where confidentiality, integrity, and availability are not violated in the presence of the deliberate threats, accidental threats, and failures'' (Tchernykh et al., 2016, p. 2).

Tying the CIA triad, as a part of the *Information Security Governance* (*ISG*), to the organization clearly indicates the significant role of top management and boards of directors in the way information security is handled in the organization (Elachgar et al., 2012). Seeing the challenges as defined by Lewis Cunningham, *"cloud computing is using the internet to access someone else's software running on someone else's hardware in someone else's data center"(*Kumar et al., 2016, p. 1496).

The challenges and threads to the confidentiality implies that unauthorized access of uses sensitive data must be detected. The threat to the confidentiality of user's sensitive data is from both internal attacker and external attacker. *Integrity* implies that any violation such as data altered, data loss, or compromised should be detected. Finally, *data availability* implies that the data is inaccessible and unavailable to the consumer (Kumar et al., 2016).

A better understanding for the *Information Security Governance (ISG)* and how it reflects, as a part, the image of a good corporate governance is that it consists of the following:

- The management and leadership commitment of the board and top management towards good information security;
- The proper organizational structures for enforcing good information security;
- Full user awareness and commitment towards good information security; and
- The necessary policies, procedures, processes, technologies and compliance enforcement mechanisms

''Cooperating and working together to ensure that the confidentiality, integrity and availability (CIA) of the company's electronic assets (data, information, software, hardware, people etc) are maintained'' (Elachgar et al., 2012, p. 167). This shows how the information governance involves everyone and how information security can impact on the corporate policies (Elachgar et al., 2012).

However, there have been views that the security of these three factors of information is important as they always been, but the triangle model of the CIA does not permit the changing environment of the IT industry (Whitman and Mattord, 2009).

2.6 Cloud migration

Cloud migration refers to a series of tasks performed to migrate an application into the cloud environment. (Wang et al., 2016) The migration to the cloud is the process where a company or organization move completely their IT assets or some of them to the cloud. Khajeh et al. (2011) stated that the decision-making process for service migration can be done with two following tools:

- Cost modeling
- Benefits & risk assessment.

Cost modelling: There are several uncertain costs which the organization should be aware of such as the actual resources consumed by a system. Those are determined by its load; the deployment options used by a system, which can affect its costs, for example data transfers are more expensive between clouds compared to data transfers within clouds; and cloud providers' prices, which can change at short notice (Khajeh et al., 2011). This is beside the normal costs which can be calculated in a spreadsheet, example: IT infrastructure, data center equipment and real estate, software licenses, systems engineering and software changes, staff costs etc.

Benefits and risk assessment: Benefits and risks can be difficult or meaningless to quantify indirect cost savings, of the improved time-to-market or flexibility provided by using public IaaS clouds. Benefits can see as an advantage to the enterprise over its status quo, provided by using public IaaS clouds and on the other hand risk as the *"combination of the probability of an event and its consequence"* (Khajeh et al., 2011, p. 542). Other benefits of cloud migration, is to use the business resources in an efficient way. The opportunity of immediate scalability when required without unnecessary cost, by implementing virtualization, is a reason for businesses to implement cloud platforms. The increasing of data execution time is also a reason an organization moves to the cloud, due to reduced hardware cost and faster access. Cloud platforms also offers data storage and recovery in the cloud, in case of security breaches (Aleem and Sprott, 2012). Risk assessment is an important part of the security management systems and *''generally identifies threat paths between assets and potential threats"* (Saadat et al., 2014, p. 222).

To initiate the migration process there are many frameworks which can support and clarify the steps and tasks needed to adopt and migrate to the cloud. Among those frameworks is *decision framework* for cloud migration, which is described in *figure 2.5* and which can be separated as three steps (Kundra, 2011, p.11):

- Selecting services to move to the cloud
- Provisioning cloud services effectively
- Managing services rather than assets

In addition to benefits, there are also disadvantages of cloud computing. *Downtime* is one of the worst disadvantages of cloud computing. Since the cloud computing system are internet based, the access to it depends on the internet connection. The service-level-agreement (SLA) can impact the organization if the applications are offline. *Security and privacy* is also an important issue since

the cloud provider is managing sensitive data. Regarding the migration to the cloud, you must be prepared for different risk scenarios that may occur. The responsibility lies with cloud provider as well the organization. Limited access to data, knowledge who has access to resources and services and extended network protection with intelligence are three examples that can be considered. Since the components of cloud computing is accessible from the Internet, you must be aware of *cloud attacks*. Monitoring the movement of critical data and authenticate access to infrastructure and data can be used to minimize the risks of cloud attacks (Seshachala, 2015).

Select	Provision	Manage
• Identify which IT services to move and when - Identify sources of value for cloud migration: efficiency, agility, innovation - Determine cloud readiness: Security, market, availability, readiness, and technology lifecycle	• Aggregate demand at department level where possible • Ensure interoperability and integration with IT portfolio • Contract effectively to ensure agency needs are met • Realize value by repurposing or decommissioning legacy assets and redeploying freed resources	• Shift IT mindset from assets to services • Build new skills sets as required • Actively monitor SLAs to ensure compliance and continuous improvement • Re-evaluate vendor and service models periodically to maximize benefits and minimize risks

Figure 2.5: Decision Framework for Cloud Migration (Kundra, 2011)

2.7 Literature overview

Between advantages and disadvantages, migrating to the cloud increases organizations efficiency and offers several benefits of storing data in the cloud. However, organizations need to keep in mind the downsides of migrating, which can result the failure to move to the cloud. Security and flexibility are two of several important factors that makes an organization choose to migrate. Nowadays, organizations choose to have their confidential information stored in a way that cannot be accessed by everyone.

Relevant theory has been used in the research study to get a deeper understanding of the cloud. Facts about the cloud are generally described, then specified to the security area and migration to the cloud, which the study chooses to focus on. The produced literature, together with the related studies within the research field, will then be used to analyze the results from the data collection to draw different parallels and interpretations.

As this research is an interpretive study it intends to investigate the perceptions of the cloud consumer towards CIA during the migration process, which uses a qualitative methodology. By using this theory, it will be helpful when conducting the analysis of the findings in the final chapters, especially in the discussion chapter.

Chapter 3

3. Research Methodology

In this chapter, the methodological tradition and methodological approach are discussed. Methods of the data collection and data analysis along with the validity, reliability and ethical considerations for the research study are also presented.

3.1 Methodological tradition

Epistemology refers to the assumptions about knowledge and how this knowledge can be acquired (Myers, 1997). Orlikowski and Baroudi (1991) claims there are three paradigms based on epistemology within IS research - *positivist*, *critical* and *interpretive*. *Positivistic* researchers are assuming that *"reality is objectively given and can be described by measurable properties"* (Myers, 1997, p. 5). Myers (1997) also states that *interpretive* researchers are carried out if the access to reality is socially constructed. He also claims that *critical* researchers state that reality is historically created, which is produced by people.

Interpretive research paradigm makes it easier for the researcher to understand the human thinking and its actions in organizational and social contexts (Walsham, 1993). The paradigm for our research is *interpretive*, since we intend to focus on the security risks of the CIA and how the cloud consumer perceives cloud security based on those risks. This paradigm is suitable for qualitative studies, which is in line with our choice to conduct interviews in this research study. The core concept in this paradigm focus on how the social and natural world are not similar, since reality only can be found through awareness, shared meanings, and language (Myers, 1997). The interpretive research paradigm has potential to produce understanding to information system phenomena and it tries to understand it through the meanings that people assign to them. Social aspects achieve knowledge of reality such as shared meanings, language, and considerations in the interpretive research (Klein and Myers, 1999).

3.2 Methodological approach (Quantitative/Qualitative)

Creswell (2013) states that three research approaches can be used in a research study – *quantitative, qualitative* and *mixed methods* approach. A quantitative research was designed to study natural phenomena in natural sciences. Examples of quantitative techniques are surveys, registers, and experiments (Myers, 1997). A qualitative research involves in-depth study of a phenomena, which includes the participants' aspects to try to determine the meaning of the specific phenomena (Creswell, 2014). The mixed methods approach is a method that is used in research studies to collect both quantitative and qualitative data. By integrating the two forms of data by using various patterns that may involve philosophical assumptions and theoretical frameworks (Creswell, 2013).

Since the purpose is to focus on the security risks of the CIA and how the cloud consumer perceives cloud security based on those risks, we will conduct a qualitative research as it best suits our needs. Data will be collected from participants in an environment where cloud services are being used. This will help the researchers to get a better insight on the phenomena. The reason the qualitative

approach has been chosen is to collect data from participants that are working in the cloud environment and to share their experience. The purpose of a qualitative study is to understand issues by investigating different perspectives of people in a specific situation. These types of studies explore the influence of social, cultural, and organizational context of a study. (Kaplan & Maxwell, 1994).

3.3 Methods/ Techniques for data collection

3.1.1. Qualitative research & Interviews

A qualitative research strategy means that the researcher gathers and analyzes data with emphasis on words, instead of quantification of the data. In a qualitative research strategy, it is important to investigate how individuals interpret and perceive the social reality they are involved in. It is the participant's view that is important, and the researcher strives for contextual comprehension (Bryman, 2002). In this research study, the qualitative data will be gathered through interviews.

Interviews were chosen as a method for the data collection. According to Crang and Cook (2007), there are three types of interview techniques – *structured*, *semi-structured* and *unstructured*. *Semi-structured interviews (SSI)* was chosen as an interview technique, as it was suited for investigating of the participants understanding regarding the cloud area. The interview technique contains a few questions about the main topic that generated a discussion about cloud security and migration. The produced interview questions focused on the responses of each participant and they were also free to respond open-ended to these. Thereafter, the researcher can investigate on these responses. This characterize semi-structured interviews, since the participants are asked the same questions and can be quantified and transformed (McIntosh and Morse, 2015). Based on related research in the field and literature review, seven questions for the interviews were raised regarding the research area, diving into more detailed questions on the chosen topic. The interview questions are showed in Appendix A.

Interviews were conducted with participants from different organizations that are in different parts of Sweden. These organizations are medium-large sized and are from different industries. The organizations are specialized within IT solutions, enterprise software, Internet security and IT digital workplaces and are working within the cloud. The reason those organizations were chosen due to business contacts within the chosen organizations. Therefore, we knew which persons that we wanted to interview. The information regarding the participants are described in subsection *3.3.2 Participants*.

The names of the organizations were not mentioned, since they wanted to remain anonymous in this thesis. We considered this, since it belongs to the ethical considerations, which we respected because the survey organizations wanted to remain anonymous.

3.3.2 Participants

The participants for the study were selected by using a *purposive sampling* that is a common selection in qualitative studies (Cohen, Manion and Morrison, 2007). A *purposive sampling* means that the participants are chosen based on features and experience that enables detailed investigation of what the researchers intend to explore (Ritchie and Lewis, 2003). Due to business contacts, we knew in advance who was most appropriate to interview and what organizations we should focus on. Our goal was to get information from participants who have already migrated and have several

years of experience within the area. By getting their experience, it makes it easier to get an overview of what they considered to be positive and negative, which will then be seen in the developed roadmap. This will prevent mistakes and incidents that can cost time and money for an organization.

Therefore, the selections of participants were based on their working role and the experience of working within the cloud that are listed in *Table 1*. The participants had different working roles such as *Principal R&D engineer, Backend Software Developer, Project Analyst for customization and implementation, Chief Technology Officer, Implementation Manager* and *Head of IT Operations*. They were in various parts of Sweden. Considering the probabilities of withdrawal, eight participants were chosen for this study. Out of eight participants, two of them chose not to participate in the research study. However, the size of the 6 were enough to gather information for the research.

Age and gender was not considered when selecting the participants, since we believe that it should not have any influence on the quality of the data. The participants were given freedom to answer the questions without any limitations. Choosing this method gave the opportunity to make analysis between the interviews answers and the chosen literature (Fisher, 2007).

Participants	**Working role**	**Year of experience within the cloud**
Participant A	Principal R&D engineer	1.5
Participant B	Backend Software Developer	2
Participant C	Project Analyst for customization and implementation	3
Participant D	Chief Technology Officer	3
Participant E	Implementation Manager	2
Participant F	Head of IT Operations	3.5

Table 1: Details of the participants

The day before the interviews, we sent out an informed consent where we described, for instance, the purpose of the study, the confidentiality, and the usefulness of the study (see Appendix B). Those were sent out electronically via email. Before the interviews, respondents and researchers wrote under this document to approve the produced content. Thereafter, six interviews were conducted through a video call through the communication tool Skype that is used by organizations and private user to communicate with people. It was the optimal way to conduct the interviews since the researchers were in different parts of Sweden. The time and day of each interview was decided according to the flexibility of the participants; therefore, we did not affect them to choose any specific day.

The interviews were conducted on the same week, but different days (Tuesday and Wednesday 4/4-17 & 5/4-17) through a video call through the communication tool Skype that is used by organizations and private user to communicate with people. Three interviews were conducted on Tuesday and the other three on Wednesday. Each interview lasted between 30-40 minutes. The interviews were conducted in English, since it is a common language between the participants and

the researchers. Three of the participants, A, C & F, did not provide any answer to one of the interview questions. We respected this, as it concerns the ethical considerations. This also made the transcription of the interviews easier. The interviews were recorded, which made it easier for the researchers to focus on the interview. The audio recording made it possible to return to the transcriptions to analyze more and to pick out citations that was said during the interviews. The transcription was documented as a report. To strengthen the reliability, each interview report was sent to the participant to verify whether it was transcribed correctly. Data backup was also taken to avoid losing the collected data.

3.4 Data Analysis

The data that were collected from the interviews were analyzed using thematic analysis to translate them from raw data to categories, as shown in *figure 3.4*. According to Lichtman (2013), this is called the three C:s of analysis – coding to categorizing and then to concepts. We followed Lichtman's (2013) six step description to analyze the collected data:

1. Initial coding
2. Remove redundancies and rename list of the initial coding
3. Categorization of codes
4. Modify initial lists
5. Identification of relevant categories and sub categories
6. Move from categories to concepts

The audio recordings from the interviews were randomly divided into two groups and each researcher of the research study transcribed one of these groups. This was done close to the actuals interviews as possible. The interviews were also coded by the same researcher that transcribed them. Each researcher also wrote down the recorded information for each interview in a word-document. Then we made an initial coding of words of the participants as Lichtman (2013) is suggesting. Large amount of codes was developed from the interviews. Thereafter, it was checked for redundancies and repetitive codes were excluded. Most of the codes were not relevant for the research study; therefore, we chose to exclude those. After excluding irrelevant and repetitive codes, we managed to reduce the number of identified codes from the initial list of codes. Then, we created categories of the generated codes.

We discussed and modified the created categories to create subcategories, which resulted into that certain codes became the main topic of the category and the others became subsets within the categories. This procedure was repeated by us until all unimportant categories and were excluded till the most relevant categories were identified. The same procedure was made for the subcategories. We searched for different patterns to move from categories to concepts.

We used Microsoft Word and its comment function to mark the text with codes and find codes to ultimately categorize them later in the analysis step. They were classified by putting together codes that we considered belong to the same category. Using a sketch format can be helpful in finding different patterns and concepts, as we did (Rubin and Rubin, 1995). The developed concepts are used in empirical section and the discussion section

Figure 3.4: Thematic analysis process example

3.5 Validity and Reliability of the Research

Validity and reliability are two important perspectives when doing any kind of research. The results must be valid and reliable, as Silverman (2013, p.301) states the *"validity is another word for truth"* and *"reliability refers to degree of consistency".* This means that *validity* present how stable our suppositions are and if they are trustworthy. *Reliability* means how logical the decisions are being made during a research where the focus is on the analytical part of it. The attempts have been made to use *"the refutability principle"* and *"the constant comparative method"* that Silverman (2013, p. 301). We did the following to ensure the reliability and validity of the research:

- Semi-structured interviews were conducted with six participants to get information of their experience of migrating to the cloud.
- Participants with several years of experience of working with the cloud and the migration to the cloud were selected for the interview
- Complementary interviews were conducted to get accurate data
- The collected data from the interviews were transcribed and confirmed with the participants to increase the credibility.

According to Jootun et al. (2009, p. 42), *reflexivity* is also aspect of qualitative research apart from reliability and validity that *"relates to the degree of influence that the researcher exerts, either intentionally or unintentionally, on the findings".* Jootun et al. (2009) also states that collected data and the analysis of the data can be affected by the researchers' identities and roles. We made the analysis and the interpretation of the collected data with a caution.

3.6 Ethical considerations

It is important to consider ethics for all participants when you are working with a research. According to Jacobsen (2002) there are several aspects that the researcher should think of when performing a study:

- Informed consent
- Privacy

Ethical consideration can also be described as more important in qualitative studies as we are interacting with people as the subjects (Eide and Kahn, 2008). Creswell (2014) claims that ethical issues should be discussed before conducting the research – in the beginning, during the data collections and analysis and in the report of the research.

The participants that volunteered in the research and were aware of the risks in the participation. The purpose of the research was presented for the participants and that it was voluntary to participate. It was important that the participants were aware of what was going to happen. The participants and the researchers signed an *informed consent* before the interviews (see *Appendix B*). The research purpose and the background information were explained to the participants and we also asked for their permission of recording the interviews. The name of the participants was not revealed in the research study and they were aware of the anonymity of their interviews. The participant had also the opportunity to cancel the interview at any time or skip a question that they felt was uncomfortable.

Participators have also the right to privacy. It is important that no personal information is disclosed otherwise an approval will be needed. The participants were informed that the information from the interviews was only used for academic purposes. The gathered information was shared with each participant to ensure correctness of the transcriptions.

Chapter 4

4. Empirical Work

This chapter will present the results that was collected from the semi-structured interviews. They will be presented and divided into concepts.

4.1 Empirical findings

Several concepts were found through analysis and transcriptions of the collected data:

- A focus on security issues
- Aspects of migrating to the cloud
- Strategic security changes
- Managing and identifying risks
- Understanding the CIA model

Concept 1 – A focus on security issues

All participants agreed that security is an important part of migration, especially when you want to have access to the data wherever you are. The stored data should also be secure and unavailable to unauthorized persons.

Participant E described that the cloud can face threats which can occur in traditional networks. It is important that you have been informed of the latest information and you have a clear dialogue about what to do to minimize the risk of a security breach.

"If an organization's confidential data ends with the competitor due to insufficient routines, then we have lost our place in the IT industry" (Participant E)

Participant A stated that the security aspects of cloud services are still an issue that needs to be improved further. Security is good but should be strengthened because the technology and its developments are improved. Everything is becoming more digital and therefore it is important to strengthen security, while developing various cloud services to prevent unauthorized persons, both internally and externally, to access confidential data.

"I am not sure I would entrust any important or confidential data to be stored on the cloud." (Participant A)

Participant D claimed that we are moving towards a more digitized society and that security is an important factor around the digitalization. If you are ISO-certified according to 27001, you already have an existing approach to security work in general. The difference in this case is that you need to develop processes and frameworks and adjust it after the cloud and the migration to it.

"If you have a base to work on, you can customize the way of working to minimize the security risks" (Participant D)

The knowledge regarding the security is limited based on the experience, but Participant B thought that communication between all involved staff is important to ensure that information is not lost. Training for the staff in the field of security, which are involved in the migration, can be a key factor in being aware of possible risks and how to fix them.

"By focusing on preventing threats and risks, can the migration work be completed without any errors" (Participant B)

Participant C described that the information should be encrypted while it is used by the cloud services. Then you can be sure that the information that is provided, is not visible and cannot affect the organization in a negative way.

"To make sure who is doing what and who has special privileges, is a way to make sure that the work is not going wrong" (Participant C)

Participant F stated that the focus on the security is the key to a successful migration. It is important to lay several steps ahead and anticipate what may happen and how the specific incident may affect the migration.

"If we lose access to the IT infrastructure because of a drop-off, we need to have a backup-plan to continue work"
(Participant F)

Security is a crucial factor, especially in a migration project. The data storage should only be accessed by authorized persons, especially if the data is accessible from anywhere. Before and during the migration, it is important to communicate and participate with employees to minimize security breaches. Being proactive is essential to predict the worst-case scenario regarding security issues and lay several steps ahead. As we are going towards a more digitized society, the security must be improved and become a primary focus. Sharing knowledge and improve communication can have a positive impact on migration and usage. Encrypting the data and securing it to comply with the organization's rules and policies.

Concept 2 – Aspects of migrating to the cloud

According to Participant A, the infrastructure is already in place and it is much easier to use a finished product for storage than to build one from scratch. Migration to cloud will facilitate it for the organization by making it easier, since they do not have to worry about maintenance and updates when it is operational.

"Migration to the cloud can lower the costs and simplify maintenance of the data storage"
(Participant A)

Participant E stated that a migration is necessary due to legacy systems. Organizations lacks functionalities and workflows and need better tools to provide this. A cloud solution creates future growth, security, functionality, and the ability to adapt in the future. It is also cost effective. Even if an organization have a positive approach overall, the uncertainty of how it will look-and-feel is

always a struggle. Through communication and information, an organization tries to undermine this feeling as much as possible.

"Thorough analysis of current systems and structure is a crucial prior of a migration, or when changing any type of system. "(Participant E)

Participant E continued to describe that before migrating, you must gather information of daily users across the company so that all topics, issues and requirements are covered. This can be done with the advantage of live interviews, with users from different departments. Every single person is not needed, but people with key roles or within key areas are most likely to participate. In addition to analysis, information is very important. To inform the organization prior to, during and after the change, increases understanding of what is going on and the willingness to participates.

"Getting everyone in the same direction is extremely important, and a positive approach greatly facilitates. "(Participant E)

Participant B claimed that there were several points that needed to be taken into consideration before migrating to the cloud. The first thing was to decide on a cloud provider by comparing other providers. Participant B thought that following questions were important:

- How do they compare to competition when it comes to security?
- How big is their focus on security, what is their selling point? Is it high-end security or is it user-convenience?
- Have they had any security breaches in the past? If yes, how did they handle it?

"Make sure to maintain a close dialog with the cloud provider. It is good to have direct contact with technical support in order to tackle technical issues fast" (Participant B)

Thereafter, a dialogue with different organizations that have done the same transition must be conducted to get first-hand information of the experience and the domain specific challenges that they faced.

Participant D stated that a migration to the cloud will increase the availability of the data, since you can access it from anywhere. As Participant D described it, there are several steps to be taken into consideration before a migration. How will the cloud provider keep data safe, what backup options will be available, will the customers approve if data is stored outside of Sweden? A migration to the cloud will reduce operational costs and increase IT effectiveness.

"Using cloud will drive change and development of IT services faster as customers together facing similar difficulties and problems in on-prem hosting. "(Participant D)

According to Participant B, being able to migrate to the cloud, means that there is a good separation of concerns in the product or service that is being developed. Separating or decoupling the infrastructure from the software that runs it, makes the system scalable and easily mouldable.

"I think that it is a positive sign for a company that has started with internally hosted infrastructure to be able to move on to the cloud" (Participant B)

Hence there is really no need for organizations to keep developing their own infrastructure if there is a provider that can provide the same or more capabilities for a lower price, according to Participant B.

"It is a relief for the company to be able to completely focus on the product or service they are developing" (Participant B)

Beside more effective maintenance and operational costs, cloud present giving your information and data to others to store them for you. This can raise questions about how trustable their service provider and how they are compliant with the security and handling of data internally and externally, according to Participant C.

"Cloud provide a unique opportunity for companies to reduce the cost of running their own servers." (Participant C)

Participant C stated that before migrating, you should know which data that will be migrated to the cloud, and if there is a need to make adjustment to the data format before migrating. As well as what the risks are and how sensitive the data migrated to the cloud to the company.

"It is important to ensure having a backup for all the migrated data in case something went wrong" (Participant C)

Before migrating to the cloud, you first need to figure out what you want to accomplish with the migration. It is important to analyze how a migration can affect the company, both in positive and negative aspects. But also, how the daily work of the staff can be affected. A migration to the cloud reduces the operational costs and you do not need to put resources on deploying it on your own server, according to participant F.

"By outsourcing operations to an external partner, which will reduce spending resources" (Participant F)

An analysis must be done to see how a migration can impact the organization. Several factors must be taken into consideration before migrating to the cloud. Employees and resources are examples of factors to ensure risk management and future risk control (proactiveness). A cloud solution is effective in an economical perspective and create growth and functionally to the organization. Therefore, the organization needs also to be informed before, during and after about the changes and updates being made to get a better understanding of the cloud. The critical point to highlight among the others, the selection of the cloud provider and how trustworthy and complained with the security focus they are, as well the previous experiences and continuous improvement from older knowledge.

Concept 3 – Strategic security changes

Participant D stated that you might need to add and address new areas as the data is outside of your own control. Even if it is outside the country, you must ensure that you have the correct rules and policy's covering that. If something goes wrong, you need to know what you will do about it.

"Using the right cloud provider with secure thinking and knowledge but innovative agenda, will help you keep an updated and modern security policy's "(Participant D)

Participant E described that cloud can change an organization strategy regarding security. Therefore, the participant listed several factors such as *two-factor authentication, mobile device management, encryption, stronger password policy* and *mindset.*

"Due to the availability, some additional security measures may be necessary" (Participant E)

The cloud may result in the organization no longer have direct access to the code that runs the infrastructure, according to Participant B. The participant also claimed that the way they maintain close contact and relations with the cloud providers, will result into quicker technical support in case of breaches or potential threats.

"Migrating to the cloud should force the company to consider finding ways to partner up with the cloud provider" (Participant B)

Participant C thought that the cloud can impact the organization's strategies. By providing more collaboration and easy access for data and information globally allow the business to develop and be more onsite where they can support their customers.

"This needs a reflection on the internal security auditing process and strategies" (Participant C)

Participant F states that a focus on the security perspective can get an organization to change direction and prioritize the security work. More resources are being put on training staff, which is good for an organization in a marketing perspective, but also can lead to new contacts and customers within the area.

"By prioritizing security, you ensure that routines and processes are followed to be classified as a secure organization on the market" (Participant F)

The cloud can affect an organization strategy regarding security, according to Participant A. Routines and processes must be documented so that the organization has the basis to go back to if problems arise. Especially if you want to have control on your own information.

"Updated guidelines must be in place to have control of the process from start to the end" (Participant A)

The organizations' strategies can be affected by migrating to the cloud. Data will be stored in cloud, and different accesses needs to be set up. New routines and processes needs to be clarified and shared in case of an emergency and adjusted according to the new strategies impacted by the migration. Adjusting those can generate continuous improvement on the security side and

development of the organization and its work, improving the staff's skills by providing them with resources can lead to establishment with new business areas and customers.

Concept 4 - Managing and identifying risks

Based on the CIA triad, there are several risks that can be acquired during the migration process. Participant E described that *integrity* contains risks such as data adaptation between the new and the old system.

"The data will need a lot of adaptation between the old and the new system. This can be done by careful work, but it is also a significant risk if something goes wrong or is missed out" (Participant E)

Participant D added that separation of the data can get accessed to the wrong user data is also a risk within the *integrity*.

"If the cloud provider does not separate the data in the right way you might get access to the wrong user data and the other way around" (Participant D)

Participant D stated that giving one user all responsibility is a risk for the *availability.*

"By putting all data in someone else's responsibility is a danger, but making the correct decision of provider will decrease it" (Participant D)

Participant E believed that cloud generates *availability* for the user but can also be a risk by having the availability over various places.

"The cloud generates great availability for the user. It is also a greater risk to have this availability scattered all over various places, due to the possibility for the user to work everywhere "(Participant E)

Participant E also stated that by moving data to cloud can also result to a risk within the *confidentiality* in several business cases.

"Moving data to the cloud could be a risk in some future business cases, if it does not comply with the potential customer, especially in a global market" (Participant E)

Participant B described that the most basic aspect that should be considered during migration is *availability*, depending on how the migration process is designed and implemented.

"The easiest way to do migration is to shut down all systems, move the running software and the data to another physical location and start all systems again" (Participant B)

By having the data that is in transit can be compromised in some way. This can happen in diverse ways. This case can potentially affect the *confidentiality and integrity* of the data being transferred.

"Unsecured channels, like unencrypted HTTP connections, moving data outside of an VPN can affect confidentiality and integrity" (Participant B)

Participant B continued stating that loss of data may also occur during migration, as an *integrity* of data security aspect. It may not happen as simply as it sounds, like losing data in transit, because the data will still exist at the source.

"This problem can be mitigated quite simply by keeping a backup of all the data for an X amount of time" (Participant B)

Risks raised during the migration can occur and have a negative impact on the process, form the view of the CIA model, moving the data between two systems can create and impact the business and causes loss in the data and the access to it. Hanging between adopting the data between old and new systems while running; and shutting down the system and moving; Managing those risks early and creating a clear plan, such as backup, can save time and resources from a view and from another, it can allow a smooth and effective transformation without impacting the daily work in the organization. The decision can be left to the compliance policies and how the organization is managing the risk.

Concept 5 – Understanding the CIA model

Participant D thought that the CIA Triad covers all aspects from a big perspective.

"Focus on the data confidentiality and the personal integrity from a person's view and also from the availability side of when, how and where to get access"
(Participant D)

Participant E described that everything can be covered within the CIA, but what also was important, and not covered, was the culture of the company. The culture is the foundation of the business and will affect every step taken.

"A migration (or any other project) must be matched with the business and its culture, only then you will know how to proceed." (Participant E)

The knowledge regarding the security is limited based on the experience, but Participant B thought that the CIA covers the security aspects.

"The CIA triad covers well the security aspects that a company is concerned with and that the company may eventually bear responsibility for" (Participant B)

Participant C described that the CIA is a good concept and covering most of the security issues related to the cloud. It was basically established for data centers before the cloud took place, nowadays the auditing and accountability is new things where CIA where not covering before.

"The challenges and risks raise for sure the CIA will need to expand toward new directions."
(Participant C)

The CIA triad covers all parts of the cloud, but also IT security in general. But that is not the most important, since other factors such as staff and culture must synchronize to get a working environment, according to participant A.

"The CIA triad is a good way of predicting what may happen, but which is also constantly evolving" (Participant A)

Participant F described that the CIA triad provides information and factors that can help you, but also the organization, when it comes to improving security in different contexts. Encryption, access control and data backups are a couple of obvious examples of factors that you use when working with cloud services.

"Since security is constantly evolving, we can expect new technologies in the near future. So, take advantage of the CIA triad" (Participant F)

The CIA model is seen from two views, a model which is covering all aspects of the security in the cloud, allowing the organization to predict and being proactive toward what's coming, and another who sees that there are missing factors in the model need to be added such as compliance to the organization culture and policies. From another point of view, some mentioned that the model is working well however as new technologies rise and developed, we will need to expand the model toward new horizons.

4.2 Empirical overview

In this section, we are summarizing the information and data we gathered during the interviews and organizing it in a meaningful way to have a better view and understanding for the migration process and related security issues from the CIA triad perspective. Part of our focus was to interview individuals who gained knowledge and experience from their work with cloud migration.

We have collected common points used or expressed during the interviews to give an overview and better understanding, where each concept shares one or more of those points. It was important to highlight the issues facing the security and how the simplicity of using the cloud can result in a negative impact to migrate. All of that was directed into understanding and absorb the changes on the security and how to identify the risks and managing them to minimize the current and future challenges; working to build trust between the stakeholder as an initial step toward effective migration and continuous improvement. Being proactive and focus on early initiatives, training and culture can be a key toward preventing security risks.

As a result, we found that the following points were essential and agreed upon by most of the interviewees:

1. Knowledge sharing and Relationship (Trust)
2. Risk management and Proactive
3. Compliance
4. Continuous improvement

Each element was mentioned or stated during the interviews as a citation, one way or another, a given example: *"A migration (or any other project) must be matched with the business and its culture, only then you will know how to proceed."* This is seen from the perspective of Compliance. Another example is *"Make sure to maintain a close dialog with the cloud provider. It is good to have direct contact with technical support to tackle technical issues fast"* which is seen from the view of knowledge and trust.

Those points will be discussed in chapter 5 *''Discussion''* to link them to the literature review and contribute to the roadmap.

Chapter 5

5. Discussion

The aim of the study was to investigate the cloud security, with a focus on the security risks of confidentiality, integrity and accessibility and how the cloud consumer perceives cloud security based on those risks.

This section will be based on the collected data from the semi-structured interviews. The result of the data collection will also be analyzed and related to the literature review. Therefore, the section will be based on the concepts.

Research questions for the study:

- *How the consumers perceive the cloud security in terms of confidentiality, integrity and availability, in the migration process?*

- Which elements to consider for a successful migration from security perspective?

5.1 A focus on security issues

The participants perceived that cloud security plays a major role for the organization, as both the staff and the organization can be positively or negatively affected, depending on what happens when you migrate to the cloud. As Participant E described it, the cloud can face different threats that occurs on regular networks, such as confidential data ends with the competitor. This can happen to organizations by not having complete routines of how to act if this occurs. Zanella (2010) is supporting this by referring to security requirements, by making duplications of the controls in the cloud environment. Therefore, it is important that data and access control are included in the duplications.

"*The most important cloud entity, and the principal quality driver and constraining influence is the consumer"* Vouk (2008). However, the consumer does not need to create or maintain the security services, since it is the cloud providers task to support the security services. It is supposed to be an effective method to control the security and privacy issues (Zanella, 2010). According to Participant A, the cloud security aspects are currently an issue, that needs further improvements due to technology and its improvements. Therefore, there is a negative and incomplete aspect of the storing confidential data in the cloud from the participant's perspective.

Moving towards a digitized society also requires that the security is continuously checked for improvement. The participants see this as a required demand to maintain good security before and while migrating. As Islam et al. (2014) is describing in the literature, security and privacy issues are the most important concerns that can hinder the migration decision.

In addition to technical factors, it is important that the communication with the involved staff is proactive. Training for the involved in the field of security is important, because you can identify and prevent risks quickly in the early stage of the migration. Kalloniatis et al. (2014) confirms this

by describing that organizations must make choices that is related to their services and operational procedure into the cloud, together with the risk assessment practice resulting.

Information needs to be encrypted while the cloud services use it. In this case, the information that is provided is not visible and cannot affect the organization negatively. Focus on the security compliance and being proactive are the key to a successful migration, according to one of the participant's. It is important to lay several steps ahead and anticipate what may happen and how the specific incident may affect the migration. By identifying risks and potential threats, an organization that is migrating to the cloud can prevent these, since the risk assessment is a part of security management (Saadat et al., 2014).

5.2 Aspects of migrating to the cloud

Migration to cloud will facilitate for the organization by making it easier, since they do not have to worry about maintenance and updates when it is operational. The infrastructure is already in place and it is much easier to use a finished product for storage than to build one from scratch. Organizations lacks functions and processes and thus need tools to maintain a structured IT infrastructure. By using a cloud solution, an organization will result in a future growth, security and functionality, since the cloud provider maintains and corrects security measures, which is also cost effective. Khajeh et al. (2011) describes that organizations should be aware of the resources that is consumed by a system, but also what can affect their costs. Examples of costs are the services from the cloud providers and data transfers. The theory described from Khajed et al. (2011) complies with the answers we received from the participants, since they also considered that costs and bought services to minimal.

Before migrating, information must be gathered from the users so all topics, security issues and requirements are covered. It is important that the staff's ideas, knowledge and experience are gathered before the migration decision is initiated. This is done by interviews with the users from different departments. To inform the organization prior to, during and after the change, increases understanding of what's going on and the willingness to participates. Several points need also to be taken into consideration before migrating to the cloud. The first point is to decide on a cloud provider by comparing other providers to create a sense of trust. The security concerns are the most important factors, taking into consideration how the cloud provider compare competition when it comes to security, how big the focus on security is and if there have been any security breaches in the past. Kundra (2011) mentions, in his decision framework for cloud migration, several aspects that needs to be take into consideration before migrating. You need to identify which IT services to move and when and identify sources of value for cloud migration. Efficiency and innovation are examples of two sources of value. This also result in a changed IT mindset such as monitoring SLAs to ensure continuous improvement.

A migration to the cloud will increase the availability of the data, since you can access it from anywhere. As the participant describes it, there are several steps to be taken into consideration before a migration. How will the cloud provider keep data safe, what backup options will be available, will the customers approve if data is stored offshore, for example *''outside of Sweden''*? A migration to the cloud will reduce operational costs and increase IT effectiveness. Cloud will drive change and development of IT services faster as customers together facing similar difficulties and problems in on-prem hosting. It is also important to analyze how a migration can affect the company, both in positive and negative aspects. As well, how the daily work of the staff can be

affected. A migration to the cloud reduces the operational costs and you do not need to put resources on deploying it on your own servers. It is not necessary for an organization to operate and develop its own IT infrastructure if there is a provider that can offer the same service at a fixed cost. By using the SaaS service model, the organization can use its applications on the cloud infrastructure. Using a web browser to access, the organization does not need to maintain the operating systems or the network. This reduces the operational costs and increases the IT efficiently for organizations by having a fixed cost (Ramgovind et al., 2010).

5.3 Strategic security changes

The organizations may need to add and address new areas, as the data is outside their own control. Even if it is outside the country and they must ensure having the correct rules and policy's covering that. Using the right cloud provider with secure thinking and knowledge as well innovative agenda, will help the organization to be compliance and keep an updated and modern security policy's. The cloud can change some organization strategies regarding security. Due to the availability, some additional security measure may be necessary such as two-factor authentication, mobile device management, encryption, stronger password policy and mindset. By using the private cloud deployment model, the cloud provider owns the data and maintains it. It is also easier to manage security and upgrades since the organization have more control over the use. The services are available for the users at the organizational level, compared to the public cloud, where the provider manages all the resources and applications (Jadeja and Moldi, 2012).

The close contact and relations with the cloud providers, will result into quicker technical support in case of breaches or potential threats. Migrating to the cloud should allow the organization to consider finding ways to collaborate with the cloud provider. By providing more collaboration and easy access for data and information globally can allow the organization to develop and be more onsite where they can support their customers (Kundra, 2011). Routines and processes must be documented so the organization has the basis to go back in case problems arise, especially if you want to have control on your own information. Updated guidelines must be in place to have control of the process from start to the end. The organizational policies will be affected and changed when making IT changes. Necessary procedures, policies and processes for the organization’s assets (data, information, staff, software, hardware) needs to be revised to ensure that the organization maintains the CIA (Elachgar et al., 2012).

5.4 Managing and identifying risks

There are several risks that can be acquired during the migration process. *Integrity* contains risks such as data adaptation between the new and the old system. There is a risk that data may be lost during the migration process, therefore, it is important that there is a backup for all data. In connection with a migration, some customization may need to be made. This can be done by careful work so that nothing goes wrong or is missed out (Tchernykh et al., 2016).

Unsecured channels, like unencrypted HTTP connections or data transfers outside of an VPN can affect the moving of data, which concerns the *confidentiality* and integrity. To simplify the migration, all current systems must be shut down, then move the software and data to another physical location and then restart all systems (Kumar et al., 2016).

The cloud can be distributed over various location. A positive matter is that it makes it possible for the users to work and get access everywhere. If one user is responsible for the cloud migration, it is a risk for the *availability*. The user can then control permissions and do more than necessary (Kumar et al., 2016).

5.5 Understanding the CIA model

The CIA triad covers all aspects of the cloud. By focusing on the data confidentiality and the personal integrity from a person's view and from the availability side of when, how and where to get access. Another concern is the compliance culture of the organization. The culture is the foundation of the business and will affect every step taken. A migration must be matched with the business and its culture, only then you will know how to proceed.

The CIA is established for data centers before the cloud took place, nowadays auditing and accountability are new matters the CIA were not covering before. It also provides information and factors that can help the organization, when it comes to improving security in different contexts. Encryption, access control and data backups are a couple of obvious examples of factors that can be used when working with cloud services. The client does not need to create and maintain security services in the cloud environment. Data will still belong to the client. This is an effective method to control security issues within the cloud (Zanella, 2010).

There are several threats to the CIA, the threat of confidentiality of user's sensitive data can come from internal and external attackers. By detecting data loss in early stages implies on the integrity. Availability implies that data is not accessible and unavailable to the consumer. These are the challenges and threats that can occur (Kumar et al., 2016).

5.6 Discussion overview

It is worth mentioning that trust, risk management and proactive; compliance and continuous improvement were used in the discussion as shared elements between the concepts. Those elements allowed us to build a view toward the security plan in a more detailed way based on the collected data from the interviews and the related articles. The elements can give the consumer as view on the stages needed and surrounding the migration process, starting from the early stages where CIA risks and challenges are identified till the security plan is build and the migration is completed, see *figure 5.1*.

Those four points can be described as following:

- Knowledge sharing and Relationship (Trust) between the consumer and other stakeholder is important, as the consumer need to have a full trust and competence how the stakeholders will ensure the security and handle the organization data (Ashish and Kakali, 2017). This is reflected by Elachgar et al. (2012) about the involvement of the stakeholders and the importance of trust and knowledge sharing.

- Risk management and Proactive is about monitoring the system flow such as critical data and authenticate access to the infrastructure to minimize the risks of cloud (Seshachala,

2015). Beside allowing to have training and webinars to create new mindsets and skills to increase the sense of security inside the organization (Zanella, 2010).

- Compliance – The organization and its business culture are important to understand during a migration. Involved persons needs to set up guidelines and deadlines how the work is going to be done and how the information is going to be disseminated within the organization. In addition to the information that is disseminated internally, continuous dialogues must be done with external factors that are involved in the migration, to prevent issues that arise and thus keep the time schedule (Kundra 2011).

- Continuous improvement is the process of following and updating the cloud against current and future risks, ensure that the system ahead of any issues which can cause failure or damage to the data or downtime with the system impacting the SLAs (Kundra 2011).

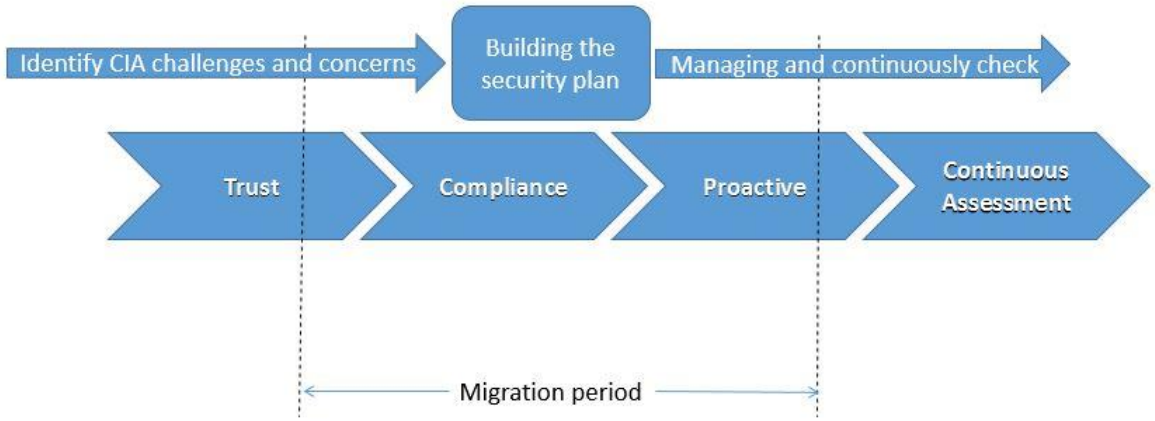

Figure 5.1: Cloud migration roadmap from cloud security aspect

5.7 Reflections on the discussion

According to the collected data from the articles and interviews we could find an interesting outcome highlighting the possibilities for risk, and how it can impact the organizational decision to migrate. It is important as well to mention the benefits resulting from migrating and how it can impact the company on multilevel, but also how to proceed from start-up and fix errors that occur during the migration process.

Security issues, migration process, strategical changes, risk management and the CIA triad were the concept that were developed during the data analysis. In these concepts, we could then relate the answers that we received from the interviews. We have experience from working in the IT industry, so we could also recognize ourselves in their working methods such as pre-work, actors and end-users. The purpose of the study was to find out the focus on the security risks of confidentiality, integrity and accessibility and how the cloud consumer perceives cloud security

based on those risks. We did not compare our characteristics and experiences with the informants who participated in the study. So, any type of affection to the result was not made, since we wanted to know their perspective regarding this area. The reflexivity on the study was not impacted, we have used a neutral way to collect the data to ensure that our roles in the IT field will not impact the answers or the ideas of the interviewees. Working on this research has allowed us to gain more knowledge and experience which will be useful for our careers.

Chapter 6

6. Conclusion

This chapter will present the conclusion on the whole research. In addition to that, future research and the contribution are also presented in this chapter.

6.1 Conclusion

Among many challenges facing the migration, the security has always been a focal point and a high concern from the cloud consumers. This research focused on security issues and risks facing organizations and companies planning to move towards cloud solutions. Cloud security is a major concern for the decision to migrate, as both the staff and the organization can be positively or negatively affected. The CIA triad assisted in giving a wide coverage on how to identify and recognize the security risks and challenges. However as there are more changes and major advances in the cloud technology, it was important to investigate and identify the elements the consumer need to understand and keep in focus before, during and after the migration.

The research intended to find out the focus on the security risks of confidentiality, integrity and accessibility and how the cloud consumer perceives cloud security based on those risks. By using persons with experience within the cloud area, the research questions could be answered. The qualitative research methodology was adopted to understand the cloud area. Semi-structured interviews with 6 persons from different organizations were used a data collection technique.

Therefore, we have focused on answering the following questions:

- *How the consumers perceive the cloud security in terms of confidentiality, integrity and availability, in the migration process?*

- Which elements to consider for a successful migration from security perspective?

Based on the findings, a roadmap was developed consist of four elements which can support in the migration decision. Those elements are: *Trust, Compliance, Proactive* and *Continuous assessment*. *Trust* and *Compliance* will allow the cloud provider to understand and analyze the consumer's concerns regarding security and build a plan which integrate solutions addressing those concerns.

This will follow by *Proactive* and *Continuous assessment*, with more involvement from the consumer to advise the provider with the security strategy and continuous assessments either internally or through an auditing company as a 3rd party.

Tying those 4 elements to the CIA triad we can get a better understanding on how to create strategies, processes identifying and managing risks, and provide the consumer with a wider view to manage issues related to the confidentiality, integrity and availability.

The security plan roadmap will assist the consumer to get a better understanding on the relationships, issues and process which need to be recognized pre, during and after the migration. The plan will assist the consumer to establish a framework structure to serve as a support and guidance; and how to work with different stakeholders.

6.2 Contribution

This dissertation contributes to the area of cloud migration and related security issues from the perspective of the consumer with a focus on the CIA triad. We worked to clarify and establish a roadmap to support and guide the stakeholder in general and the cloud consumer specifically to assist in the decision to migrate to the cloud and during the work on building the security plan.

The cloud area is a wide area to research in, since it consists of many perspectives, which makes it interesting. The field of research is usually found in the IT context. However, it is not just limited to IT.

Organizations depend more and more on cloud services to provide greater security, access to data where they are and storage capabilities, to make work easier. Cloud computing studies have been done at a general level, where no security has been touched on in a detailed level.

On the other hand, most studies about the cloud are both quantitative and qualitative studies, where the focus is on the technical aspects. This research is focused on the security risks of CIA and how the cloud consumer perceives cloud security based on those risks. However, we have also tried to have a deeper understanding on the risks and the cloud consumer to gain knowledge.

As the result indicates, developing a roadmap containing four elements can support an organization in the migration decision. This also allows the provider to understand and analyse the consumer's concerns regarding security and build a plan which integrate solutions addressing those concerns.

This research contributed to the more in depth understanding of the cloud security and the challenges facing the consumer in the decision to migrate from the perspective of the CIA. As well the elements surrounding the process to build a security plan, and how those elements can assist the stakeholders in general and the consumer specifically to understand how to deal with those challenges.

Furthermore, the outcome from the research is applicable for the improvement of the CIA model to adopt to new future challenges and assist the stakeholder to gain a wider view on the cloud migration and security risks that might raise. Those findings can help the organizations to better understand the cloud and security issues and assist in the decision making to migrate.

6.3 Author's contribution

There are two authors for this research study – *Khaled Tawfique* and *Arlind Vejseli*. During the writing, the work has been divided equally and closely worked together. Arlind Vejseli focused more on writing the *Methodology section* and Khaled Tawfique focused more on the *Introduction section.* The *Literature review* were divided among the authors, so both had as much focus in this chapter. It is difficult to determine how much work has been made by each of the people on the

writing, as both writers are equally responsible for this research study. Both authors have discussed and reviewed each other's work on all chapters. However, both authors were involved in the *data collection*, *data analysis* and the *empirical findings*. In the remaining chapters of the research study, both authors were involved finalizing these.

6.4 Future research

In the future, this research study can be further explored by including another cloud stakeholder such as the cloud provider and cloud auditing and their role in supporting and building trust and compliance in addressing the challenges and concerns related to the consumer's security. Another extend for the study is the CIA triad and how to create an agile model to include the future rising challenges which are not included in the current model.

Another research area that can be investigated in is the trust in cloud computing. By focusing on the security perspective, privacy and security can be used to measure the trustworthiness of cloud computing. By using participants from two or more organizations, a comparison between those organizations can be made to get relevant answers for the study.

References

Aleem, A. and Ryan Sprott, C. (2012) 'Let me in the cloud: analysis of the benefit and risk assessment of cloud platform', Journal of Financial Crime, 20(1), pp. 6–24. doi: 10.1108/13590791311287337.

Baraković, S. and Husić, J. B. (2016) 'Short and sweet: Cloud computing and its security', in 2016 11th International Symposium on Telecommunications, BIHTEL 2016. doi: 10.1109/BIHTEL.2016.7775725.

Bojanova, I. and Samba, A. (2011) 'Analysis of Cloud Computing Delivery Architecture Models', 2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications, pp. 453–458. doi: 10.1109/WAINA.2011.74.

Buyya, R., Broberg, J. and Goscinski, A. (2011) Cloud Computing: Principles and Paradigms, Cloud Computing: Principles and Paradigms. doi: 10.1002/9780470940105.

Bryman, A.(2002). *Samhällsvetenskapliga metoder*. Malmö: Liber

Carroll, M., van der Merwe, A. and Kotze, P. (2011) 'Secure cloud computing: Benefits, risks and controls', Information Security South Africa (ISSA), 2011, pp. 1–9. doi: 10.1109/ISSA.2011.6027519.

Carter, S. M. and Little, M. (2007) 'Justifying knowledge, justifying method, taking action: Epistemologies, methodologies, and methods in qualitative research', Qualitative Health Research, 17(10), pp. 1316–1328. doi: 10.1177/1049732307306927.

Chandran, S. and Angepat, M. (2010) 'Cloud Computing: Analyzing the risks involved in cloud computing environments', Proceedings of Natural Sciences and Engineering, pp. 1–6.

Cohen, L. et al. (2007) 'Research methods in education', books.google.com. Available at: http://books.google.com/books?hl=en&lr=&id=i-YKKgtngiMC&oi=fnd&pg=PR17&dq=%22Research+methods+in+education%22&ots=zV3AD2JHdF&sig=4KHwespHfeMKxd1ZpYHxArmGhoo.

Crang, M. and Cook, I. (2007). *Doing Ethnographies*. SAGE Publications Ltd.

Creswell, J. W. (2013) Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, Research design Qualitative quantitative and mixed methods approaches. doi: 10.1007/s13398-014-0173-7.2.

Creswell, J. W. (2014) Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, Research design Qualitative quantitative and mixed methods approaches. doi: 10.1007/s13398-014-0173-7.2.

Eide, P. and Kahn, D. (2008) 'Ethical issues in the qualitative researcher-participant relationship', Nursing Ethics, 15(2), pp. 199–207. doi: 10.1177/0969733007086018.

Elachgar, H. et al. (2012) 'Information security, 4TH wave', Journal of Theoretical and Applied Information Technology, 43(1), pp. 1–7. doi: 10.1016/j.cose.2006.03.004.

Fisher, C. (2007). *Researching and Writing a Dissertation*. Essex: Prentice Hall.

Gartner (2017) 'Gartner Says Worldwide Public Cloud Services Market to Grow 18 Percent in 2017', Gartner Research, 8, pp. 1–5. Available at: http://www.gartner.com/newsroom/id/3616417. [Accessed: 2017-03-08]

Hasan, F. (2011). *Demystifying Cloud Computing*. Faculty of Computers and Information, Mansoura University, Egypt.

Hassan, T., James B.D. and Gail, J-A. (2010). Computing definition and features. *IEEE Security & Privacy*, volume 8, nov-dec 2010.

Islam, S., Weippl, E. R., and Krombholz, K. (2014). A Decision Framework Model for Migration into Cloud. *Proceedings of the 16th International Conference on Information Integration and Web-Based Applications & Services - iiWAS '14*, (2012), 185–189.

Ismail, U. M., Islam, S. and Mouratidis, H. (2015) 'Cloud security audit for migration and continuous monitoring', in Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015, pp. 1081–1087. doi: 10.1109/Trustcom.2015.486.

Jacobsen, D. I. (2002). *Vad, hur och varför?: Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen.* Studentlitteratur AB, Lund

Jadeja, Y. and Modi, K. (2012) 'Cloud computing - Concepts, architecture and challenges', in 2012 International Conference on Computing, Electronics and Electrical Technologies, ICCEET 2012, pp. 877–880. doi: 10.1109/ICCEET.2012.6203873.

Jootun, D., McGhee, G. and Marland, G. R. (2009) 'Reflexivity: promoting rigour in qualitative research', *Nursing Standard*, 23(23), pp. 42–46. doi: 10.7748/ns2009.02.23.23.42.c6800.

Kalloniatis, C. *et al.* (2014) 'Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts', *Computer Standards and Interfaces*, 36(4), pp. 759–775. doi: 10.1016/j.csi.2013.12.010.

Kapil, R and Kelvin Ng (2015). *Best Practices for Mitigating Risks in Virtualized Environments*, (April), Cloud Security Alliance 1–35. https://downloads.cloudsecurityalliance.org/whitepapers/Best_Practices_for_Mitigating_Risks_Virtual_Environments_April2015_4-1-15_GLM5.pdf [Accessed: 2017-03-29]

Kaplan, B. and Maxwell, J. A. (1994) Qualitative research methods for evaluating computer Information Systems, Qualitative Research Methods.

Khajeh-Hosseini, A. et al. (2011) 'Decision support tools for cloud migration in the enterprise', in Proceedings - 2011 IEEE 4th International Conference on Cloud Computing, CLOUD 2011, pp. 541–548. doi: 10.1109/CLOUD.2011.59.

Kilström, T. (2016). *Factors limiting adoption of new technology: a study of drawbacks affecting transition from on-premise systems to cloud computing.* Master thesis, Industrial Engineering and Management. Stockholm: Kungens Tekniska Högskola.

Kissel, R. (2013). *NIST: Glossary of Key Information Security Terms.* http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf [Accessed: 2017-04-25]

Klein, H. K. and Myers, M. D. (1999) 'A Set of principles for Conducting and Evaluating Interpretative Field Studies in Information Systems', MIS Quarterly, 23, pp. 67–93. doi: 10.2307/249410.

Konrad, A. (2016). *Spotify Moving Onto Google Cloud Is A Big Win For Google Over Amazon And Microsoft.* https://www.forbes.com/sites/alexkonrad/2016/02/23/spotify-is-a-big-win-for-google-cloud/#419676b574b9 [Accessed: 2017-03-08]

Kumar, M. *et al.* (2016) 'Data outsourcing: A threat to confidentiality, integrity, and availability', in *Proceedings of the 2015 International Conference on Green Computing and Internet of Things, ICGCIoT 2015*, pp. 1496–1501. doi: 10.1109/ICGCIoT.2015.7380703.

Kundra, V. (2011). Federal cloud computing strategy. White House: Washington. https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf [Accessed: 2017-05-02]

Lichtman, M. (2013). *Qualitative Research In Education: A User's Guide*. 3rd ed. Thousand Oaks: SAGE Publications.

Liu, F. et al. (2011) 'NIST Cloud Computing Reference Architecture Recommendations of the National Institute of Standards and', NIST Special Publication 500-292, 292(9), p. 35. doi: 500-299.

Malluhi, Q. and Khan, K.M. (2011). Cloud computing without seeing. *Proceedings of the First International Workshop: Security & Privacy Preserving in e-Societies*; p42-44.

McIntosh, M. J. and Morse, J. M. (2015) 'Situating and Constructing Diversity in Semi-Structured Interviews', *Global Qualitative Nursing Research*, 2, p. 233339361559767. doi: 10.1177/2333393615597674.

Mell, P. and Grance, T. (2011) 'The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology', *Nist Special Publication*, 145, p. 7. doi: 10.1136/emj.2010.096966. Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [Accessed: 2017-02-12].

Myers, M. (1997) 'Qualitative research in information systems', *MIS Quarterly*, 21(2), pp. 241–242. doi: 10.2307/249422.

NIST (2013) Glossary of key information security terms, NIST IR. doi: 10.6028/NIST.IR.7298r2.

Oracle (2012). *Cloud Reference Architecture.* Oracle Enterprise Transformation Solutions Series. http://www.oracle.com/technetwork/topics/entarch/oracle-wp-cloud-ref-arch-1883533.pdf [Accessed: 2017-02-20].

Orlikowski, W. J. and Baroudi, J. J. (1991) 'Studying Information Tech- nology in Organizations: Research Approaches and Assump- tions', *Information Systems Research*, 2, pp. 1–28.

Posey, B. (2013). *To cloud or not the cloud: What's your cloud migration strategy?* http://searchcloudcomputing.techtarget.com/feature/To-cloud-or-not-to-cloud-Whats-your-cloud-migration-strategy [Accessed: 2017-04-08]

Prasad, A., Green, P. and Heales, J. (2014) 'On governance structures for the cloud computing services and assessing their effectiveness', International Journal of Accounting Information Systems, 15(4), pp. 335–356. doi: 10.1016/j.accinf.2014.05.005.

Prendergast T. (2016). *Top cloud security trends for 2016.* http://www.datacenterjournal.com/top-cloud-security-trends-for-2016/ [Accessed: 2017-03-08]

Ramgovind, S., Eloff, M. and Smith, E. (2010) 'The management of security in Cloud computing' IEEE International Conference on Cloud Computing.

Ritchie, J. and Lewis, J. (2003) Qualitative Research Practice: A Guide for Social Science Students and Researchers, SAGE Publications.

Rubin, H, and Rubin, I 1995, *Qualitative Interviewing : The Art Of Hearing Data*, n.p.: Thousand Oaks : Sage, cop. 1995.

Saadat, S. and Shahriari, H. R. (2014) 'Towards a process-oriented framework for improving trust and security in migration to cloud', in 2014 11th International ISC Conference on Information Security and Cryptology, ISCISC 2014, pp. 220–225. doi: 10.1109/ISCISC.2014.6994051.

Seshachala, S. (2015). *Disadvantages of cloud-computing.* https://cloudacademy.com/blog/disadvantages-of-cloud-computing/ [Accessed 2017-09-15]

Shields, A. (2014). *Must-know: Cloud computing services and deployment models.* http://marketrealist.com/2014/07/must-know-cloud-computing-services-and-models/ [Accessed 2017-11-05]

Singh, A. and Chatterjee, K. (2017) 'Cloud security issues and challenges: A survey', Journal of Network and Computer Applications, pp. 88–115. doi: 10.1016/j.jnca.2016.11.027.

Silverman, D. (2013). *Doing qualitative research*. 4th ed. London: SAGE.

Singh, S., Jeong, Y. S. and Park, J. H. (2016) 'A survey on cloud computing security: Issues, threats, and solutions', Journal of Network and Computer Applications, 75, pp. 200–222. doi: 10.1016/j.jnca.2016.09.002.

Tchernykh, A. et al. (2016) 'Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability', Journal of Computational Science. doi: 10.1016/j.jocs.2016.11.011.

Thao, T. P. and Omote, K. (2016) 'ELAR' : Extremely Lightweight Auditing and Repairing for Cloud Security', ACM International Conference Proceeding Series, 5, pp. 40–51. doi: 10.1145/2991079.2991082.

Theoharidou, M. et al. (2013) 'Privacy risk, security, accountability in the cloud', in Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom, pp. 177–184. doi: 10.1109/CloudCom.2013.31.

Tieto Corporation. (2014). *The cloud story in an infographic nutshell.* https://www.slideshare.net/TietoCorporation/what-canclouddoforyouwhitepapertieto [Accessed: 2015-05-10]

Walsham, G. (1993) 'Interpreting Information Systems in Organizations', Organization Studies, 15, p. 269. doi: 10.1177/017084069401500614.

Wang, C. W. and Chang, S. E. (2016) 'Cloud service in stock trading game: Service virtualization, integration and financial application', in International Conference on Ubiquitous and Future Networks, ICUFN, pp. 857–862. doi: 10.1109/ICUFN.2016.7537158.

Wolff, J. (2017). *The Good and Bad News About Cloudbleed.* http://www.slate.com/articles/technology/future_tense/2017/02/the_good_and_bad_news_about_cloudbleed.html [Accessed: 2017-03-07]

Whitman, M.E. and Mattord, H.J. (2009) *Principles of information security*. 3rd ed. Thompson Course Technology; 2009.

Vouk, M. A. (2008) 'Cloud computing - Issues, research and implementations', in Proceedings of the International Conference on Information Technology Interfaces, ITI, pp. 31–40. doi: 10.1109/ITI.2008.4588381.

Yigitbasioglu, O. M. (2015) 'External auditors' perceptions of cloud computing adoption in Australia', International Journal of Accounting Information Systems, 18, pp. 46–62. doi: 10.1016/j.accinf.2015.09.001.

Zanella, R. (2010). *Cloud Security and Governance: Who's on Your Cloud?*. Ely: IT Governance Publishing 2010.

Appendices

Appendix A - Interview Questions

Our purpose is to investigate the cloud security, with a focus on confidentiality, integrity and availability in the migration process, from the perspective of the Cloud Consumer. Understanding and identifying those elements can assist in avoiding the failure and enhance the success of the migration process.

This study is conducted by Arlind Vejseli and Khaled Attalla, who studies the master's program in Information Systems at Linnaeus University in Växjö. The study is part of our master's degree in informatics at the master level.

*CIA Triad, represent Confidentiality, Integrity and Availability, is a model designed to guide policies for information security within an organization.

Thanks for sharing part of your time and experience with us.

Introduction

- What is your position at work?
- How long have you been working in the organization under cloud and security issues regards to the cloud?

Cloud Services and Security

- Before migrating to the cloud platform, what are the essential steps to be taken into consideration by users?
- What do you think, as a cloud consumer, of migrating to the cloud? Do you find any positive and/or negative aspects of this?
- Can you identify 3-5 risks based on the CIA Triad which can be acquired during the migration process? And how is each one of those risks relevant to the CIA? (Ex. Risk 1 is relevant or impacting C, I or A)
- How can the cloud change/impact the company's strategies regarding the security?
- Do you think that the CIA Triad is covering all aspects concerning cloud security? Why/Why not?

Appendix B – Informed Consent

Consent form for participation in a research study (Adopted from: CODEX, Rules and Guidelines for research, 2016, *Informed Consent* [online] Available at: http://www.codex.vr.se/en/manniska2.shtml [Accessed: 2017-05-01]).

Title/Topic*:* Decision to migrate to the Cloud
A focus on security from the consumer perspective

Date: Feb 2018

Contact information to the researchers
Arlind Vejseli
Mail: av222dm@student.lnu.se
Phone number: +46 72 177 01 93
City: Växjö

Khaled Tawfique
Mail: kt222dr@student.lnu.se
Phone number: +46 73 595 91 29
City: Västerås

Research purpose
More organizations choose to migrate to the cloud, it is important that this is done in a way where the security risks are minimal. The purpose of the study is to focus on the security risks of confidentiality, integrity and accessibility and how the cloud consumer perceives cloud security based on those risks. Understanding and identifying those elements can assist in avoiding the failure and enhance the success of the migration process. This research study will benefit the researchers, who intends to investigate the perceptions of the cloud consumer with cloud security, confidentiality, integrity, and availability in the migration process, from the cloud consumer's perspective. The result of this thesis will show how organizations that have not migrated to the cloud, can enhance a successful migration to the cloud. This would lead to minimal risks to enhance a failure migration to the cloud, since the results can be used to prevent a failure.

Description of the research study process
The interview questions and the date and time will be confirmed to you at least before the interview through e-mail. The interview will be conducted through Skype since we cannot meet face-to-face. The interview will be about 45-60 minutes. Based on your experience within the cloud area, you are requested to share your experiences with a focus on confidentiality, integrity and availability in the migration process, from the perspective of the Cloud Consumer. The interview will be recorded as it is a part of the data collection process. The recorded material will be used to cite certain statements but also to describe the empirical findings.

Benefits of being in the study
We will gain knowledge about the perceptions of the cloud consumer with cloud security, confidentiality, integrity, and availability in the migration process, from the cloud consumer's perspective. You will be benefitted by knowing these perceptions and can you use these in your current work, since this master thesis can be used as a roadmap.

Confidentiality
The participation in this study is anonymous, which means that your identity or your organization's identity will not be revealed. The participant's names will be described as *"Participant A, Participant B, etc"*. Therefore, your names or organization's names will not be mentioned in this Master thesis. The recorded audio will be kept in USB drive and the notes from the interview will be documented in a Word document. Only Arlind and Khaled (researchers) will have access to this material. You will receive a copy of the recorded interview where you can confirm that what you said is correct. The recording audio will be used when writing the empirical findings sections and the analysis. All material regarding the interview will be deleted after the Master thesis is completed.

The right to refuse
Your participation in this study is optional. You can, at any time, refuse your participation in the study without explanation. Participation will also not affect your relationship with the researchers, either private or in working life. If you feel uncomfortable responding to one or more questions, you are entitled not to answer the question. If you choose to cancel the interview, we will delete all information about you and your experiences with immediate effect.

Further questions about the research
If you have any questions about the research or about your role in the research study, please contact Arlind Vejseli (av222dm@student.lnu.se) and Khaled Tawfique (kt222dr@student.lnu.se) by mail.

Consent
Your signature confirms that you choose to participate in our research study and that you have taken note of the above information. You will get a signed and dated copy of this form electronic.

Signature
I consent to participate in the research study *"Cloud Migration Framework and Roadmap: A focus on the security and the confidentiality, integrity and availability triad from the consumer perspective."* conducted by Arlind Vejseli and Khaled Tawfique.

_____ *Participant*	_____ *Arlind Vejseli & Khaled Tawfique*