Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

UNIVERSITY OF TWENTE.

Tom Hendrixen

the way we see it

Secure Cloud Computing in the Dutch Financial Service Market

Master Thesis Business Information Technology

People matter, results count.

Secure Cloud Computing in the Financial Services Market

Master Thesis Business Information Technology

v1.0

T.F.M. (Tom) Hendrixen
s0211168
University of Twente, the Netherlands
& Capgemini, the Netherlands

May 24, 2011

Contact

Author

Name: *T.F.M. Hendrixen*
Function: Graduate Student University of Twente, Capgemini;
Address: Weteringweg 1, 7076BL, Varsselder-Veldhunten, The Netherlands
Phone: +31-636113932
Email: thomas.hendrixen@capgemini.com

Graduation Committee

First supervisor

Name: *dr. ir. M.J. van Sinderen*
Phone: +31 53 - 4893677
E-mail: m.j.vansinderen@utwente.nl

Second supervisor

Name: *prof. dr. J. van Hillegersberg*
Phone: +31 53 - 4893513
E-mail: j.vanhillegersberg@utwente.nl

First external supervisor

Name: *H. Groenwold*;
Phone: +31 30 - 6894766
E-mail: harmen.groenwold@capgemini.com

Second external supervisor

Name: *ir. R. Zubcevic*;
Phone: +31 30 - 6896897
E-mail: rene.zubcevic@capgemini.com

Management Summary

This document describes a research about security in cloud computing for the financial services market. This research is performed by Tom Hendrixen, a graduate student at the University of Twente (UT). The research took 6 months and was started on the 1st of November 2010. The research is conducted for the Financial Service (FS) Global Business Unit (GBU) of Capgemini NL which is orientating to put cloud technology into the market.

The main subject of this research is security in public cloud computing. Public cloud computing is a new technology with characteristics such as resource pooling and elasticity to provide a base for IT services. Using cloud technology can deliver business benefits and cost reduction. Implementing this new technique does not only bring advantages, it also comes with some disadvantages such as security issues. In this thesis we concentrate on the data security disadvantages.

Security issues in public cloud computing are seen as the most important issues when implementing or services in a public cloud. In this thesis we describe the most important and most referenced data security threats found in literature. Once identified, we describe how current public cloud providers deal with these threats. Some examples of these threats are: unauthorized inside users, data location, faulty infrastructure, and denial of service.

To check if public cloud computing services can be used by companies in the FS market, we compared the data security threats in public cloud computing with the data requirements at FS companies. In chapter four of this thesis the FS requirements applicable to these services are described in more detail.

Every service demands different security requirements. For example public web blogs assign a much lower priority to security as applications such as Internet banking and other services in the FS sector. The FS sector has high security standards and uses certificates and risk analysis to ensure this. Because this thesis concentrates on the Dutch FS market, practical research in the field is done to describe the current state of public cloud computing in this market. In this thesis the practical findings are related to the findings in literature. By taking this step interesting conclusions are exposed.

Conclusions By interviewing security experts, we found that the use of public cloud computing only covers a small, almost no, part of the services used at FS companies. The used public services are implemented because they are cheaper and more agile than on premise solutions. Another interesting property is that they do not contain data that might become incompliant to legislation or might create great losses when security breaches occur.

Security is seen as a major issue when implementing public cloud solutions. With the information gathered during the research we state that moving to cloud computing is a trade-off process between costs savings, agility and security risks. The cheaper, more agile the solution the higher the security risks and the other way around.

With this trade-off between the cloud benefits and the risks, we conclude that in situations where high levels of security are required public cloud computing cannot compete with the security of on-premise traditional services. This because the 'cheaper' public cloud solutions do not fully comply with the security standards required by companies. As the public cloud deployment model provides the cheapest computing and storage capacity, security risks are high.

When taking these insights and looking at the FS market we see that the implementation of public cloud computing for core services in FS companies is not interesting. The benefits of moving to public cloud computing are not enough to accept the risks associated with the current technique. Loss of control, lack of security guarantees and trust in the provider are issues that expose risks which FS companies are not willing to take for their core services.

In some cases FSs in public cloud computing cannot be implemented because of legislation. E.g. Dutch legislation prohibits companies to store or process data in countries that demand lower security requirements to personal data. Another act in Dutch legislation requires FS companies to provide access to auditors of their information systems. Services that are applicable to this law cannot be placed into the public cloud.

Public cloud computing does become interesting in situations where risks can be accepted (partly). (E.g. non-core and supporting systems) During the research we found that the CIA framework was used by FS companies to classify the data used. With this framework, acceptance of risks per type of data is defined. By doing a risk management research at a public cloud provider a classification threshold can be set for data that may not be placed in the public cloud. With this classification organizations become able to select services that can or can't be implemented in the public cloud.

Contents

Preface

After finishing my final courses at the university, Capgemini gave me the opportunity to do an interesting graduation project in their organization. After some meetings with recruiters and passing some tests, I started my research six months ago in November. The goal of the research was to determine if data security in public cloud computing complies with the data security requirements at Dutch financial services companies.

During this research I have learned a lot about cloud computing, risk management, and the financial services sector. To gather this knowledge I referenced a lot of literature, experts, colleagues, and supervisors. Often it was hard to find information about the financial services market. Through discussions with colleagues and interviews with experts I got the information needed which pointed me into the right direction to successfully finish my research.

Now at the end of my graduation research it is time to thank the people that supported me during the process. Without them I would not have managed to bring this research to a successful and satisfying end. First of all I would like to thank my supervisors at Capgemini. Harmen and Rene provided me with the necessary expertise at the right time and brought me in contact with the experts needed for my research. Second, I would like to thank my supervisors at the University of Twente, Marten and Jos. They gave me the needed opinions, comments and support during my graduation period.

Furthermore, I would like to thank all the professionals who were willing to reserve some time to contribute to the practical part of my research.

Finally I would like to thank the people in my private environment. Without you I would not have enjoyed and succeeded as much as I did now.

I hope that you will enjoy reading this thesis and that you will be able to profit from the content of this research. When things are unclear or you have questions, please contact me.

Kind regards,

Tom Hendrixen Varsselder-Veldhunten, May 2011

1 Introduction

1.1 Background

New techniques offer new opportunities for businesses. Cloud computing is currently hyped as one of the new IT developments with high business relevance. Actually cloud computing is not a new technique since its concepts date back from the 1960's [1], but at this moment due to the maturity of the Internet finally reached a stage where it can have important practical applications. Cloud computing is seen as the technology of the future. For the Financial Services (FS) Global Business Unit (GBU) of Capgemini, cloud computing potentially creates opportunities for their clients. For example, banks and insurance companies can use cloud solutions and gain advantages from the new technique. But cloud computing does not only have advantages compared to traditional systems, there are some critical points to look at. Security is one of these critical assets for these financial service companies [2].

As the Global Business Unit Financial Services of Capgemini is interested in public cloud solutions for their clients, a research has to be done to see what opportunities are available. Capgemini is interested specifically in the public cloud because it provides the user with all the benefits the (cloud computing) business model is able to give. As security in cloud computing seems to be an important factor when choosing for the public cloud, a research about security in public cloud computing is needed.

Some questions Capgemini wants to have answered are: What data security issues should we take into consideration when developing FS solutions for the public cloud? Does the security of public cloud computing comply with the security requirements of our clients?

To be able to place financial services into the public cloud, the security of the public cloud has to comply with the security requirements demanded by the FS companies. Translating the questions of Capgemini into the main goal of this research; our aim is to determine whether data security in public cloud computing complies with the data security requirements at Dutch financial services companies.

1.1.1 Capgemini

Capgemini was founded in 1967, since then Capgemini has established itself as one of the top 5 IT services and consulting companies worldwide. Capgemini's headquarters are established in Paris. From here, Capgemini is active in over 30 countries with more than 100.000 employees in Latin-America, Europe and Asia.

Capgemini delivers value to performance and change processes of their clients by a complete and innovative offer of consulting, technology and outsourcing services. This is done in a unique way called the Collaborative Business Experience which aims at working together with clients to get faster and better results. Capgemini has three divisions [3]:

- Consulting Services - Based on knowledge of sectors and business processes Capgemini Consulting provides an addition to business transformation and economic performance of its clients.
- Technology Services - Capgemini designs and integrates technical solutions, creates innovations and transforms technical environments of clients. These services are concentrated on system architecture, integration and infrastructure.
- Outsourcing Services - Capgemini also takes responsibility for IT-management. In its wide offer of services, IT-management and price flexibility are very important. For this reason, outsourcing is one of the key activities of Capgemini.

Each of these environments is subdivided into Global Business Units (GBUs). This research is done within the Financial Services Business Unit of Technology Services.

1.1.2 Financial Services GBU

Financial Services (FS) is a department which focuses on banking, insurance and pensions. Some clients of FS are ABN AMRO, ING, RBS, Nationale-Nederlanden and Achmea. To provide its clients with the exact services they need, this global business unit is divided into several business units (responsible for generating the revenue), practices (responsible for professional growth, guiding and rewarding employees) and central staff units (HR, etc.). The research is done on behalf of the business unit Technology Development and Integration (TDI). At the moment of writing there is a restructuring of these business units, which means that names will be changed per 1 January 2011 the department name TDI will no longer be used.

The main goal of TDI is to bring together several key technology offerings under one practice. TDI supports its clients with comprehensive technology consulting services to achieve their goals. TDI's services include Architecture, IT Governance & IT Improvement, Custom Software Development, Application Management, Application and Data Migration, Business Process Management, Integration and Infrastructure Services [4].

1.2 Cloud Computing

Cloud computing is an IT term that describes a collection of collaborative technologies that provide online services. The objective of cloud computing is to move computing and data from desktop and portable PC's to large computing facilities. The term cloud computing is defined by different authors in different ways. In [5], Vaguero et al. try to define cloud computing by merging these definitions. They propose the following definition which will be used in this research:

> "Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the infrastructure provider by means of customized SLAs."

Key driving forces of cloud computing are the ubiquity of networking, falling storage costs and progressive improvements in Internet computing software. Due to these forces cloud computing is able to provide several new capabilities. For example cloud computing is able to deliver elastic capacity (CPU, storage, bandwidth). This makes cloud services scalable which provides easier capacity planning for clients than in traditional systems [6, 7]. Due to a virtualization layer, setting up a service in an existing environment becomes very easy. In a few clicks a new virtual machine is up and running [7]. This enables opportunities for businesses to quickly adapt to (changes in) the market [7]. Most cloud providers charge for the usage of the cloud resources, e.g. pay per gigabyte of network bandwidth and CPU hours consumed. Not having capital expenses (CAPEX) for data centers, software licenses, etc. creates interesting opportunities for new businesses [7].

1.3 Problem Description

In public cloud computing, information is stored in centralized places that can be located all over the world. Often these locations are unknown for the customer. In contrast to this, traditional systems store information on-premise where data location can often be specified up to the hard disk on which it is stored. Storing information in a location you do not know raises security concerns, for example storing privacy sensitive data which has to be kept inside country borders. But not only the security of storing data raises concerns. In these datacenters user actions are executed centrally, due to this privacy and security of users' actions are also subject to concern. Some example applications with security threats are resource provisioning and distributed application execution [6, 7, 8]. Using infrastructure that you do not own and control brings security issues [9]. Having your services placed in public data centers used by other parties raises another security issue called perimeter security. In traditional data centers perimeter security measures at the network border are used to keep unwanted users outside your network. In public cloud computing, there is no network border, thus perimeter security measures have to be taken at the virtual machine itself [8].

For some applications security is not a big issue. E.g. public web blogs assign a much lower priority to security than applications that use highly sensitive data such as Internet banking and other services in the FS sector. The FS sector has high security standards and uses certificates and risk analysis to ensure this [10].

Security in cloud computing is a hot topic, for example: Neelie Kroes advocates for stricter rules on border crossing data storage, which is the case in cloud computing. In her speech [11], she states: "protection of personal data is a fundamental right in Europe, when we store this data in the cloud, we take the risk of losing control of the data." To prevent this, research has to be done on security in cloud computing.

Another example comes from the International Data Corporation (IDC). In 2009, this company did a survey [12] and asked 263 IT executives to give their opinions on IT cloud services (see figure 1). Security was ranked first among the challenges and issues preventing the adoption of cloud computing [12]. In 2010 KPMG asked the same question in a survey with 125 decision makers located in the Netherlands; security issues were still ranked first. The second and third places were populated by legal and compliance issues. 63 percent of the respondents agree with the statement that security concerns are a blocking issue when it comes to cloud computing [13].

1.3.1 Problem Statement

Cloud computing affects FS companies in both ways, it reduces costs but increases risk. To gain advantages from this new technique a balance has to be found between these factors. According to literature, the data security is a major risk that reduces the growth of cloud computing [2]. In order to gain advantages of this technique in the FS market, this security risk has to be identified in order to find the right balance that enables Capgemini to create successful

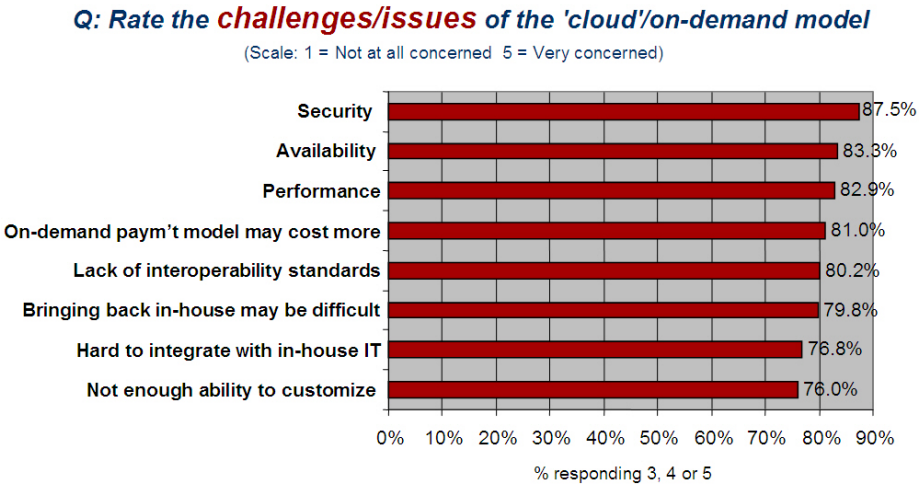

Figure 1: IDC cloud challenges 2009 [12]

business solutions. To do this, a research has to be executed.

1.4 Research Objectives

The main goal of this research is to determine if data security in public cloud computing complies with the data security requirements at Dutch financial services companies. With data security we mean: the protection of data from unauthorized modification, destruction, or disclosure to ensure its availability, confidentiality, and integrity [14].

The Global Business Unit Financial Services of Capgemini NL is interested in cloud solutions for FSs. What solutions should they offer based on cloud technologies and are these solutions secure? Based on these questions my research scope will be limited to services in the Dutch FS sector.

The goal of this research is:

To determine whether data security in public cloud computing complies with the data security requirements for IT services at Dutch financial services companies. If the compliance is only partly, determine for which financial services data security in public cloud computing is sufficient.

We created a main question based on the problem stated in the previous section, which we will answer during our research.

Does data security in public cloud computing comply with the data security requirements for IT services at Dutch financial services companies?

To answer this question, we subdivided the main question into multiple sub questions listed below:

- What are the current top data security threats in public cloud computing and how are they mitigated?
- What are the data security requirements for IT services in the Dutch financial service market?
- To what extent is cloud computing used in the Dutch financial service market?
- What are the relations between cloud computing, current data security threats and data security requirements for IT services in the Dutch financial service market?

When these questions are answered, conclusions can be drawn and the main question of the research will be answered.

1.5 Scope

To keep the research controllable, we use the following scope:

- We research the security aspects in public cloud computing only. There are different types of cloud deployment models, but as Capgemini wants to the research to be about public cloud computing, we take this scope.
- We focus specifically on services used by FS companies.
- We do not describe detailed services but keep a high abstraction level.
- This also means that we do not describe and use business specific service requirements.

1.6 Structure and Approach

The research is structured according to the techniques described by Verschuren en Doorewaard [15] and will be explained in this section. The research is divided in 4 parts which are executed in an incremental order during this thesis. The blue colored blocks present the theoretical part based on literature. The brown colored blocks present the practical part underpinned with literature. The yellow block presents the synthesis of the information gathered during the previous parts. Finally, the green blocks present the conclusions and further research.

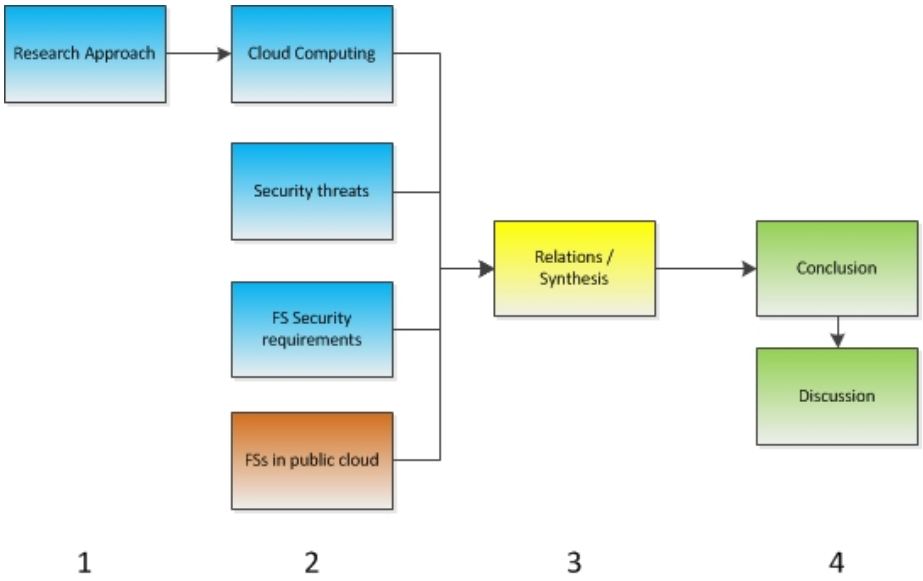

Figure 2: Research structure [15]

The first part of this thesis, see figure 2, consists of the orientation on the research topic and background. During the orientation, literature is used to get insights in security of cloud computing in the Dutch FS market. The literature used for this orientation is published by well-known sources such as Forrester, Elsevier and IEEE. The main reason for this orientation is to get extensive information about the subject and the problems which occur in the research area. The main activities in this part are: description of the problems, objectives, research questions and the approach to answer these questions.

The second part of the thesis, see figure 2, answers the first three sub questions of the research. These answers provide the foundation for the study. In this part literature is used to describe the cloud computing technique and its data security threats in more detail. To get specific information about the cloud computing technique, its threats and their mitigation, we chose to use literature published by the National Institute of Standards and Technology(NIST) and the European Network and Information Security Agency (ENISA), which are US and EU institutes that publish standards about cloud computing and its

security. For the mitigation part we used market offerings of well-known public cloud providers.

We use literature get information about the data security requirements in the Dutch FS market. Experts in the field directed us to legislation and assessments of regulators that require data security for these services. To get more theoretical insights in this field we used literature obtained by referencing legislation databases and documents published by The Dutch Bank, a Dutch FS regulator.

To get information about the current usage of cloud computing services in the FS market, a quick scan by means of an orienting questionnaire is done and interviews are held with four security experts stationed at Dutch banks and insurance companies.

The third part of this thesis, see figure 2, describes the relation between the answers found in part two. In this part of the thesis we analyze the insights gathered from literature and interviews. The new insights we gathered by analyzing the information and answering the last sub question provided us with the needed relations and information to answer the main question of the research.

In part four, the last part of the research, we summarize the insights gathered and we answer the main question of the research. Finally we describe the recommendations and further research that is needed in this research field.

To give an overview of the research activities a table is drawn, see table 1.

Research Question	**Methodology**
What are the current top data security threats in public cloud computing? And how are they mitigated?	Literature research
What are the data security requirements for IT services in the Dutch financial service market?	Literature research
To what extent is cloud computing used in the Dutch financial service market?	Survey among IT architects and Interviews with FS security experts
What are the relations between cloud computing, current data security threats and data security requirements for IT services in the Dutch financial service market?	Synthesis of questions 1,2,3

Table 1: Research methodology

1.7 Relevance

This research will provide information about the data security threats that are concerned in public cloud computing in the Dutch FS market. By doing so, this research will provide practical and theoretical perspectives to different parties. In the next two paragraphs the theoretical and practical relevance of this research are described.

Practical Relevance The practical relevance of this research is mainly for Capgemini. With the information derived with this research, the FS department of Capgemini is able to get clearer insights in the security issues and doubts that live at their clients. At best, with the results of this research they are able to underpin choices made and to be made about the placement of services into the public cloud.

Theoretical Relevance The theoretical or scientific relevance of the research contributes to theory development in comparing FS security requirements with public cloud security. Much has been published on security of cloud computing [12, 16, 17, 18, 19, 20, 21] for example in [17], Zhao *et. al.* describe the security concerns in cloud computing and proposes deployment models to ease the concerns.

In [12], a survey conducted by IDC suggests that cloud services are still in the early adoption phase. In the survey a list of cloud concerns is ranked by the respondents, the outcome shows security as the most important concern.

In [16], a platform to compose and explore cloud security is proposed. And [19] provides information about how to manage the security in cloud.

A more specific research based on data security in cloud is done by Heiser en Nicolett for Gartner [21]. In this research, they identified seven risks that customers should assess before using a cloud computing infrastructure. During this master thesis research ENISA published a report containing a decision model to choose a cloud service delivery model. The decision is based on business & legal requirements, architecture, and cloud computing threats [22].

At this moment there is a literature gap on the subject data security in public cloud computing for the FS market. Especially when looking at the Dutch FS market. This research will fill this gap to enrich the knowledge on this subject.

1.8 Outline

In this chapter of this thesis, we describe the background information, problem statement, objectives, approach and relevance of the research. Chapter two describes the cloud computing technique and its business benefits.

Chapter three is about data security threats and goes deeper into the security issues that come with public cloud computing in contrast with traditional systems.

In Chapter four we describe the requirements demanded by legislation, regulators and the FS companies that use the services.

Chapter five describes the insights gathered from the interviews with the security experts and provides answers on the sub question: To what extend is public cloud computing used in the Dutch financial service market.

Once the first three sub questions are answered, we describe the relations between the found insights by means of a synthesis in chapter six. In this chapter we describe the relations between public cloud computing, its data security threats, the requirements from the FS market and the current usage of public cloud computing in this market.

In the final chapters of this thesis, conclusions will be drawn upon the insights gathered in this research. The main question will be answered and recommendations for further research will be proposed.

2 Cloud Computing

Cloud computing is a complex technique with a lot of different deployment and service models. We use this chapter to explain the technique and its business case in more detail. In the introduction of this thesis we define cloud computing as:

> "Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs."

Reading this definition we see that cloud computing is a way of abstracting the cloud computing resource from the hardware and software where it runs on. This means a customer doesn't deal with the requirements of the platform such as maintenance, monitoring, hardware cost and datacenter space cost. Quoted from Linthicum [23] cloud computing is:

- Stuff you do not own.
- Stuff you do not maintain, at least from an infrastructure point of view.
- Stuff you do not see.
- Stuff you pay for as subscription.
- Expandable on demand.
- Reducible on demand.

Being able to use resources that you do not own or maintain reduces costs. The more resources used, the lower the cost will become through economies of scale. Cost reduction is one of the most cited benefits from cloud computing.

In the next sections we will describe the cloud computing technique and its business drivers. First a brief history of the development of cloud computing is described. Then the key characteristics, service models and deployment models will be described.

2.1 History

Cloud Computing seems to be one of the newest hypes in IT, a hype it is, but it isn't new. The concept of cloud computing already exists for over 50 years. In the 1960's J.C.R. Licklider introduced the term "intergalactic computer network" which is nowadays known as the Internet. The concept described a global interconnection of computer programs and data. The term "cloud" is used since the 1990's when providers began to use VPN services. These networks were able

to balance utilization across the network and to increase bandwidth efficiency. These aspects are similar to the aspects provided by a cloud computing environment which dynamically allocates resources to meet users demands [1].

In 1999 the UC Berkely Space Sciences Laboratory implemented a distributed computing application with computers connected over the internet. This application is known as SETI@home (Search for Extra-Terrestrial Intelligence). Others also tried their own variants of computing via the internet such as Salesforce.com. In 1999 Salesforce.com had the first practical cloud computing implementation which established the concept of delivering services via a website. This cloud was followed up by the Amazon Web Services, which was a suite delivering services such as storage, computation and human intelligence through the Amazon Mechanical Turk service. In 2006 this concept was upgraded to Elastic Compute Cloud (EC2) service. This is a service which is still known today and which is able to provide virtual computers on which users can run their own applications [1].

Nowadays the number of cloud computing providers is rising, some providers are: Salesforce.com, Amazon, Google, Microsoft, IBM, VMware, Rackspace, etc. These providers all try to create their own business models with different opportunities and applications of the cloud technology.

In [9] they state that cloud computing combines a number of already available computing concepts and technologies for Service Oriented Architecture. As can be seen in figure 3, these concepts consist out of Web 2.0, virtualization and communication infrastructure techniques. With these combined techniques, cloud computing is able to achieve: improved utilization and efficiency of service providers' infrastructure through controlled sharing of resources with different customers. In the next paragraph these key characteristics will be explained in more detail.

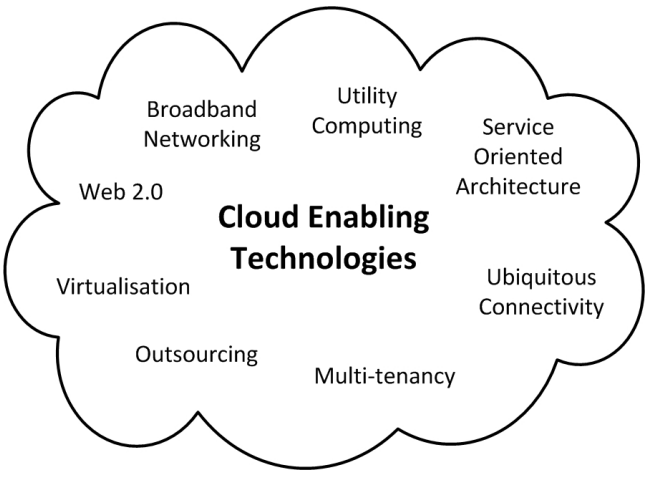

Figure 3: The Enabling techniques of cloud computing [9]

2.2 Key Characteristics

In this paragraph the key characteristics of cloud computing provided by [5, 6, 7] and [24] are summarized. This is done to give a clear view of the advantages of this technology.

On-demand Self-service Cloud resources (computing power, storage size, memory size, etc.) can be managed, added, moved, or changed by the consumer without human interaction or intervention with cloud provider personnel [7, 24].

Resource Pooling As the definition of cloud computing by Vaquero *et. al.* [5] describes; clouds are virtualized resources. Virtualization provides the power to share physical computing resources on different locations as one resource to multiple customers. This means cloud providers are able to split, assign and dynamically resize their resources to the needs of their customers. The customer does not need knowledge of the resources hardware and location [5, 24].

Broad Network Access Cloud services are accessible over the Internet, a standardized network that works with almost every platform from fat clients to mobile devices [6, 24].

Rapid Elasticity Virtualization has another big advantage, it creates elastic resources. This means resources can be scaled rapidly to the actual demand. When the demand is high, extra resources can be addressed and when the demand is low, these resources can be freed[6, 24].

Measured Service In cloud computing usage of resources can be measured. These measurements give the cloud provider input to monitor its cloud, but also create the opportunity to provide the consumer with a payment model called: pay-per-use. This means that the consumer only pays for used resources such as storage, CPU hours, bandwidth, etc. [5, 7]. For an example of this payment model we refer to appendix B.

2.3 Service models

Cloud computing has a large number of cloud service models. This number is rising because firms start providing more specialized services such as Business processes as a Service or Storage as a Service. In literature there are three service models which are the most common used and generic service models. These service models are placed in a stack called: "the cloud service model stack". A detailed scheme of this stack is depicted in figure 4 and will be explained below.

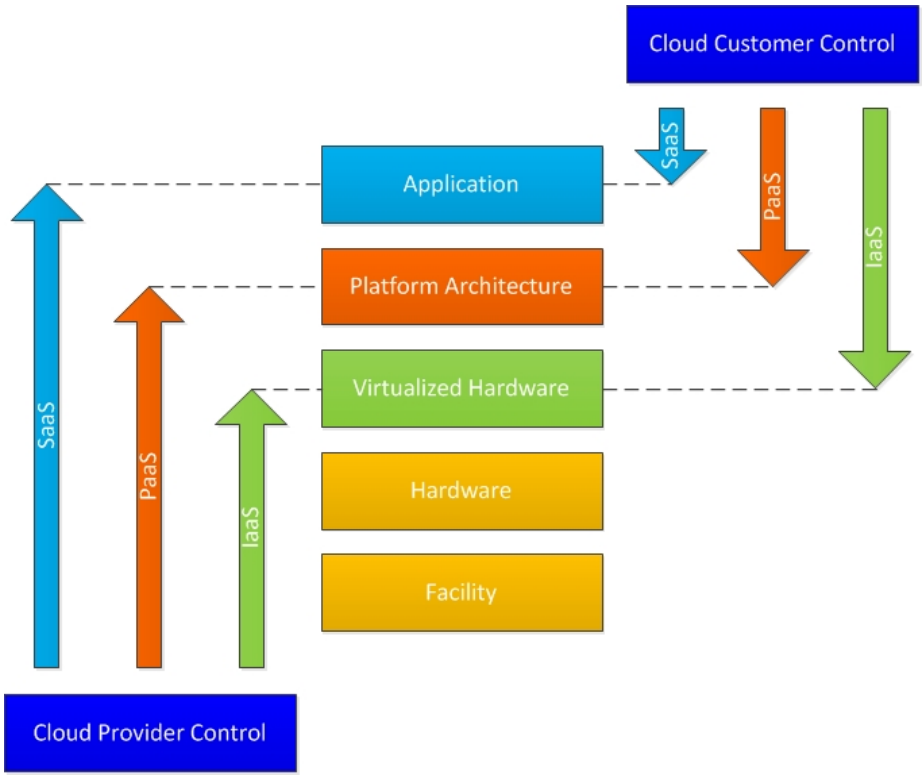

Figure 4: The cloud service model stack [25]

Infrastructure as a Service (IaaS) In the cloud service model stack infrastructure is placed in the virtualized layer which is positioned directly on the hardware. In this layer services provide standardized storage, processing power, networks and other fundamental computing resources. Services on this layer run on physical hardware like servers, storage systems, switches, routers, and other systems that handle specific types of workloads. Customers are able to deploy and run software which includes operating systems. They don't have control over the hardware except for firewalls. The security provisions on top of the basic infrastructure are carried out mainly by the customer [6, 24].

Platform as a Service (PaaS) Platform services are placed in the second layer of the cloud stack. This layer provides services with the functionality to develop, test, deploy, host and maintain applications in the same environment (the cloud). Customers develop these services based on standardized programming languages, tools and API's supported by the provider. Security provisions are shared between the cloud service provider and the customer. Customers have no control over underlying infrastructure layer where it runs on [6, 24].

Software as a Service (SaaS) Services placed in the software as a service layer are applications running on top of the cloud stack. Providers of these services are responsible for management of the applications that make use of the infrastructure which is below this layer in the cloud stack. Customers of these services do not manage or control the underlying cloud layers, which are invisible for them (see figure 4). Due to this, security provisions are carried out mainly by the cloud provider. The services are easily, consistently, and frequently accessible from different client devices by means of a standard interface such as a web browser [6, 24].

2.4 Deployment models

Cloud stacks can be deployed in multiple ways in cloud terminology these ways are called deployment models or delivery models. There are a lot of different configurations possible but to keep things easy to understand there I chose to use the four most used models of deployment in literature [9].

Public Cloud In public clouds, the cloud infrastructure is made available to the general public. Resources are shared over the Internet on a mega-scale infrastructure. The cloud itself is owned by a provider which sells cloud services [24, 26].

Private Cloud A private cloud is a cloud which is dedicated to a specific organization or group of users. Clouds like this may be managed by the organization itself or by third parties. This means that the cloud can be placed on premise and off premise. A private cloud gives the customer more control over the infrastructure and computational resources than a public cloud. [24].

Hybrid Cloud The hybrid cloud is a cloud composed out of two types of clouds public and private. These clouds are bound together so that they can exchange data. In this way the level of service and security between different applications can be adjusted. An example of this situation could be using a private cloud for high critical applications and placing the less critical applications on a public cloud [24, 26].

Community Cloud Community clouds are clouds that are used by multiple organizations that have similar objectives and concerns. (e.g. mission, security requirements, policy, and compliance considerations). Community clouds can be deployed using any of the three methods outlined above, simplifying cross-functional IT governance [24].

2.5 Business Drivers & Benefits of Public Cloud Computing

The main reasons for cloud technologies to be adopted in organizations are the pressure to decrease IT costs and to increase agility. Public clouds are large pools of resources that provide availability and reliability. Clouds can reduce CAPEX by replacing traditional hard - software systems with solutions that are scalable and flexible to adapt to changing business demands. IT cost are reduced by lowering the upfront capital expenses such as buying hardware in traditional on premise solutions [9, 22, 23]. Costs decrease by the economies of scale that occur at large cloud providers some examples are; licensing, and IT management and maintenance costs. In [27], an example is given about the cost benefits of economies of scale in datacenters. In their paper Armbrust *et. al.* describe a comparison between a medium sized datacenter (1.000 servers) and a very large datacenter (50.000 servers). The table of their comparison is shown in table 2.

Technology	**Cost in Medium-sized DC**	**Cost in Very Large DC**
Network	$95 per Mbit/sec/month	$13 per Mbit/sec/month
Storage	$2.20 per GByte / month	$0.40 per GByte / month
Administration	$\approx$ 140 Servers / Administrator	$\geq$ 1000 Servers / Administrator

Table 2: Economies of scale in 2006 for medium-sized datacenter ($\approx$1000 servers) vs. very large datacenter ($\approx$50,000 servers) [27]

In this table we see that costs of network, storage and administration decrease when the datacenter size increases. An example graph that depicts the costs changes is shown in figure 5. This datacenter size is put to the extreme in cloud computing. The number of virtual servers that are plugged in every day is approaching 90,000 for Amazon's data centres on America's East Coast alone [28].

Having the ability to only pay for what you use, small to medium sized organizations are also able to profit from economies of scale.

Moving to cloud increases flexibility, you can add as much capacity as you need, when you need it. The other way around, you can reduce the capacity just as easily. Only your spending will change. You don't have to buy enormous amounts of hardware and software in your datacenters just waiting for an opportunity to be used. Or the other way around; not being able to support your customers peak load because your hardware capacity is lacking. An illustration of this comparison is depicted in figure 6.

Installing hardware and software is done by the cloud service provider. "You can get what you need, when you need it, and with the click of a mouse" [23]. This speeds up implementations, provides business continuity, lowers management costs, shortens the time to market and transfers risks from customer to cloud provider.

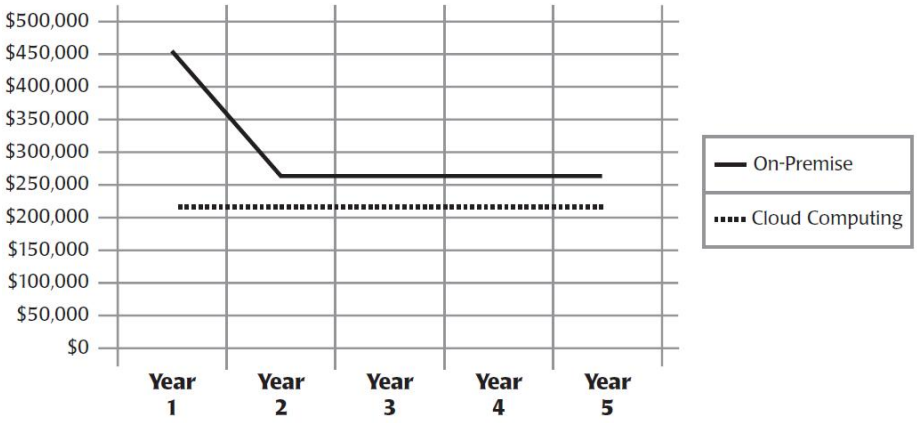

Figure 5: Example of Costs [23]

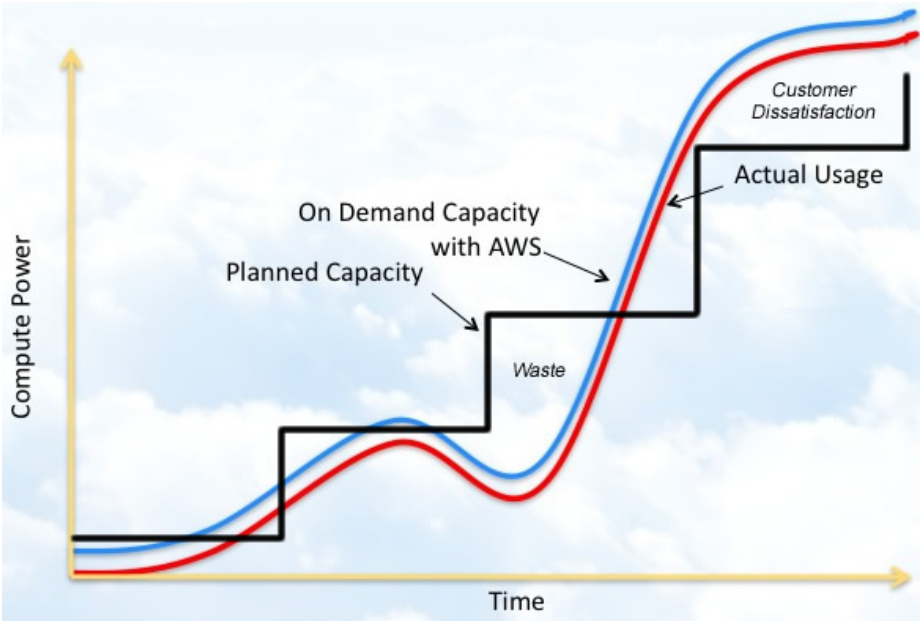

Figure 6: Capacity vs. usage in traditional and cloud computing [29]

2.6 Security in Public Cloud Computing

As already stated in the introduction of this research, security in cloud computing raises concerns at decision makers [13]. In [25], Jansen & Grance describe the following fundamental downsides on data security compared to traditional systems:

- System Complexity - A public cloud computing environment is extremely complex compared with that of a traditional datacenter. There are many components in a public cloud which provide a large attack surface. Some examples of the components that include the public cloud are: deployed applications, virtual machine monitors, guest virtual machines, data storage, and supporting middleware. But also components for self-service, resource metering, quota management, data replication and recovery, workload management, and cloud bursting. Complexity can become higher when cloud providers use other clouds to provide their resources such as infrastructure. "'Complexity typically relates inversely to security, with greater complexity giving rise to vulnerabilities"' [25].

- Shared Multi-tenant Environment - In public cloud computing resources are shared over multiple cloud customers. Sharing infrastructure with unknown outside parties may have major consequences for security. Software errors or misconfigurations may expose access to organizational data. Attackers could be cloud customers that launch attacks from inside the cloud.

- Internet-facing Services - Public cloud services are delivered over the Internet. Due to this, administrative interfaces are also exposed over the internet. Comparing this to traditional systems that were managed via intranets, extra security threats arise.

- Loss of Control - Migrating to a public cloud requires a transfer of control. Data as well as system components that were previously under the organization's direct control are now shifted to the cloud provider. The loss of control of physical and logical system aspects disables the ability to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best interest of the organization.

In chapter 3 of this thesis we will describe the security threats in public cloud computing that create these downsides in more detail. But as public cloud computing has negatives concerning security, it also has got security benefits. In [25], Jansen & Grance describe the following benefits on data security:

- Staff Specialization - Because cloud providers are large organizations, they have an opportunity for staff to specialize in security, privacy, and other concerns of high interest. With this increased specialization, staff members gain in-depth experience, take remedial actions, and make security

improvements more readily than they would have done without the specialization.

- Platform Strength - The structure of cloud computing platforms provide uniformity and homogeneity which facilitates platform hardening and enables better automation of security management activities. Some examples of these activities are configuration control, vulnerability testing, security audits, and security patching of platform components. Information assurance and security response activities also gain profit from this uniform and homogeneous infrastructure. Even system management activities gain profit, for example fault management, load balancing, and system maintenance. Finally cloud providers often meet standards for compliance and certification (e.g. PCI DSS and SAS 70).

- Resource Availability - The elastic properties which provide scalability facilitate greater availability options for cloud computing. Redundancy and disaster recovery capabilities in cloud computing environments can be used for better resilience when facing increased service demands or recovery procedures.

- Backup and Recovery - As copies of data are maintained in diverse geographic locations, backup and recovery policies and procedures may be superior to traditional services [25].

- Data Concentration - When data is only processed and maintained in the cloud, security issues with mobile devices or removable media are minimized.

3 Data security threats in public cloud computing

When implementing or moving to new techniques, management of new security threats is inevitable. This means that when implementing or moving to public cloud computing services, management of data security threats is needed. In this chapter we answer our first sub question which is: "What are the current top data security threats in public cloud computing? And how are they mitigated?"

As stated in the introduction of this research, security in cloud computing is an essential requirement. This is also the case in traditional systems which means that challenges faced by organizations planning to use cloud services are not radically different from challenges in traditional systems [9]. During this research, we assume that traditional services and cloud computing services have the same already known security threats, but can have different risks. Therefore to answer this question we will look at the threats that create additional risks in public cloud computing services compared to traditional services.

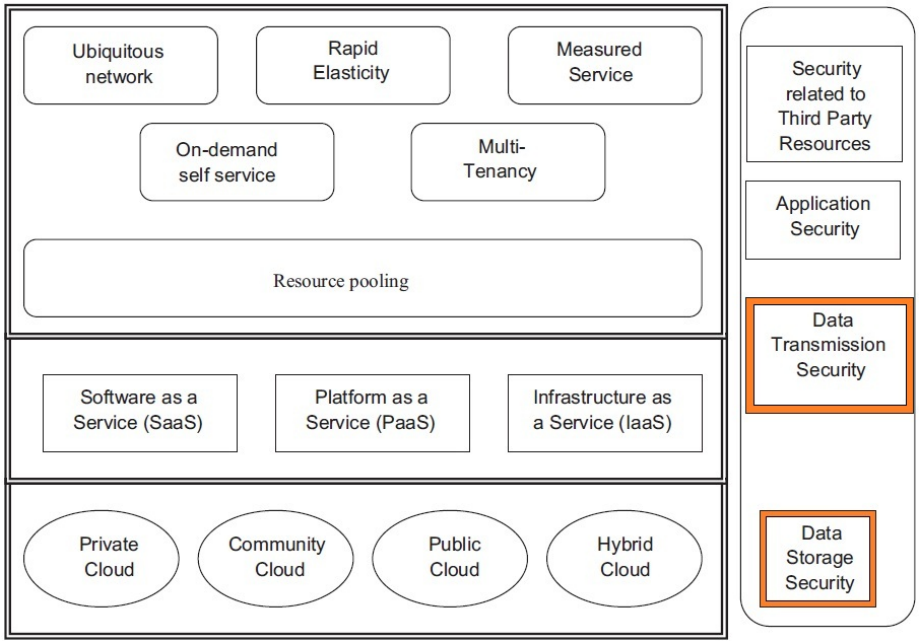

Figure 7: Security in cloud environment [2]

Each service model of the cloud computing stack requires security that is different. This difference is based on the deployment model that is used, how it is delivered and the character it exhibits. In figure 7, data storage and transmission security are depicted as fundamental security challenges for every deployment and service model in the cloud [2]. This means that data security is applicable to every service model in a cloud environment. For this reason we do not make

distinctions between service models to describe the data security threats in public cloud computing.

In the next sections we will provide the reader with the most common data security threats applicable to public cloud computing. The selected are threats most common because these are most described in literature on this subject such as: CPNI [9], Wang (Forrester) [30], and Sangroya *et al.* [31].

3.1 CIA security Model

In [9], CPNI provides an overview of threats in cloud computing. These threats are categorized according to the Confidentiality, Integrity and Availability (CIA) security model. This model is known as the CIA triad and is used as a principle of information security [32]. In figure 8 the triad with the security goals is depicted. The figure shows that when a balance between the three security goals is reached, a system is secure. But in his book Pfleeger describes that a balance is not all, the three characteristics can be independent, can overlap (see figure 8) and even be mutually exclusive.

Each security goal has its own definition. Confidentiality is defined as assurance that information is not disclosed to unauthorized persons, processes, or devices. Integrity is defined as: assurance that data is unchanged from its source and that it is not accidentally or maliciously modified, altered, or destroyed. The last side of the triad is availability which is defined as timely and reliable access to data and information services for authorized users [14, 32]. As this model provides a backbone to structure the literature findings and the data security requirements, we use it in the rest of the thesis.

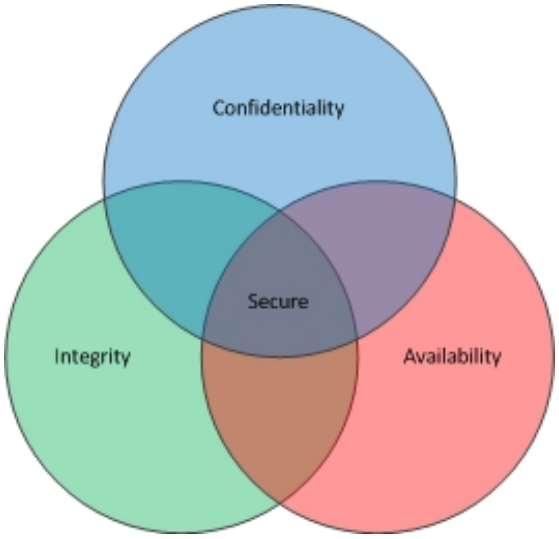

Figure 8: CIA Triad [32]

3.2 Security threats

In the next sections we describe the threats found in literature according to the CIA security model described in the previous section. We compare the vulnerabilities between cloud and traditional services. We use a simple file storage service to compare both service types with each other. In this way we are able to make a distinction between traditional and cloud services based on risks. In information security a mathematical formula is used to define risk.

Risk = threat x vulnerability x consequence.

It should be noted that the formula cannot be filled in with numeric values as you would expect from a mathematical formula. The parameters have a high abstraction level which makes them hard to define. The formula should be used to define the relation between the parameters with classifications such as low - medium - high. In this comparison, threats and consequences are constant factors, which give us the opportunity to compare the vulnerabilities between public cloud services and traditional services.

3.2.1 Confidentiality

Unauthorized inside users The first threat is ability of unauthorized inside users (providers' personnel, customers and third parties) to access data held within the cloud. Once data is stored in the cloud, cloud providers become data custodians which means, they have privileged, sometimes physical access to the data and control over the entities that can access that data. Moving from traditional in house datacenters, in which own staff has a higher trust level, to un-trusted cloud providers inside users can increase the vulnerability of the stored data [9, 33, 2].

Remote access exposure As public cloud computing provides remote (Internet) access, it also provides exposure to potential cyber attackers. This threat can be described as: external attackers that attack infrastructure, applications, hardware, software and users by social engineering (manipulating people to obtain information) [8]. Comparing the vulnerability of this threat between cloud and traditional services we see that clouds are centralized data storages. Storing data of multiple cloud customers centrally provides attackers with a richer target and thus increases the vulnerability [2]. When looking at the benefits of cloud computing, the platform strength benefit can have some advantages compared to the traditional services on this threat. Uniformity and homogeneity in the cloud facilitates platform hardening and enables better automation of security management activities [25].

Data leakage amongst other organizations In literature we found another threat: data leakage. This threat is caused by failure of security access rights across domains and the failure of data transport systems for cloud data. Data could be leaked amongst other organizations (potentially competitors) using the

same cloud provider [9, 30]. This threat is not a threat in traditional services, this because there is no data leakage to other organizations possible in the traditional service architecture.

Unknown data location Sangroya and the CPNI describe that the location of the stored data raises security concerns. When storing data, the physical location of the data and the computing resource may be under obligations. These obligations, statutory, regulatory, or contractual, may require that data is managed or disclosed in a certain way. E.g. in the US; their Patriot Act directs that any data stored on US territory must be disclosed to the government when asked for [9, 31, 34]. In traditional services, data location can be chosen by the customer himself [2]. This means that this is not a threat in traditional services.

3.2.2 Integrity

Data segregation On the integrity side of the triad, CPNI appoints data segregation as a threat in cloud computing. This threat is caused when security perimeters are defined incorrectly or when virtual machines and hypervisors are incorrectly configured. In traditional services, this is not the case because in these services (physical) perimeter security is applied [2]. Incorrect application of data segregation increases the vulnerability of the cloud service compared to traditional services. Cloud customers might even experience security breaches that should have been limited to a single customer [8, 9, 34].

User access management User access management is another subject which can lead to threats on the integrity side. If access control procedures are poorly implemented many threat opportunities arise. Unauthorized users may be able to access, modify or delete important data. An example is former employees which still have access to resources. Compared to traditional services, the only difference is that ex-employees were not selected by the traditional company, but by the outsourcer. This vulnerability could also arise in traditional systems [9, 33].

Data quality Data quality may suffer by the implementation of faulty or miss configured infrastructure components implemented by other cloud users sharing the same infrastructure [9, 30]. In traditional systems, miss-configured infrastructure can still be the case, but this is only caused by own staff and not by other users which share the same infrastructure in the datacenter. In the comparison this means that the cloud service has a higher vulnerability on integrity of data on this threat.

Secure deletion Secure deletion of data is another security risk which is much cited in literature. Cloud providers have service level objectives and give guaranties about the availability of data. They provide this high level by storing multiple copies of the data. When cloud customers want data to be deleted,

cloud-based storage may fail to delete data at all points in its lifecycle [9, 30, 33]. Compared to traditional services, data lifecycle management is controlled by the company itself and is clear. A counterargument is found in [25]. The NIST describes that staff specialization and improved backup management at cloud provider are benefits compared to traditional services. These benefits can make deletion procedures superior to traditional procedures.

Limited monitoring possibilities Cloud infrastructure technologies are designed to place a security perimeter between the cloud service and the cloud user. But with this perimeter security, insider threats and attacks cannot be out ruled. In his research Kaufman states: "Because dormant machines can't perform malware scans, they're highly susceptible to malware attacks [8]." To secure the data affected by this threat, traditional systems use e-investigations and protective monitoring. For effective protective monitoring of cloud-based information, integration between monitoring tools used by cloud providers and by cloud users is required. Tracing actions back to users and administrators requires integrated or federated identity management and logging of individuals accessing cloud resources[34]. Invoking these e-investigation procedures within the cloud can be limited by the cloud delivery model and the access and complexity of the hardware [31]. It is not possible to deploy monitoring systems on infrastructure not owned by the customer. In this way customers must rely on systems provided by the cloud provider to support their investigations because accurate information is vital in investigating incidents [9].

3.2.3 Availability

On the last side of the triad, literature describes the following threats concerning availability.

Change management Cloud providers have an increasing responsibility in change management. These changes (of software, hardware, and infrastructure) could introduce negative availability effects such as downtime. Downtime due to change management is also the case in traditional services. The only difference is that in traditional systems the customer controls the change management instead of the cloud service provider. An advantage on this threat is that at cloud providers the staff is specialized in these procedures and there are resources available for redundancy and disaster recovery procedures [9, 33, 25].

Denial of Service Wang and the CPNI describe another threat which is applicable to both, traditional and cloud services. It is the availability issue that arises when the cloud service is not available to deliver the peak load. The denial of service (DoS) threat, network bandwidth distributed DoS, DNS DoS, application DoS and data DoS are possible threats which decrease the availability of a service [9, 30]. As often stated cloud services have elastic capacity, this doesn't mean that it's unlimited. A well planned (D)DoS will still decrease the

availability of a cloud service. The vulnerability of this threat compared to a traditional system can be seen higher because different customers use the same infrastructure. If one of these customers uses all the bandwidth of computing power, the others are affected too. When comparing both, we see that clouds have a slight advantage because of the specialized staff, load balancing tools and available resources [25].

Physical disruption Disruption of cloud services or WAN providers through physical access is also a threat. Centralized datacenters should have resiliency strategies and should be secured physically. Cloud services and traditional services need the same physical security, looking at the threat at a single cloud datacenter, the vulnerability of this threat is higher because these centers are rich targets for attackers [9]. Looking at the availability of the services, we see that clouds and traditional datacenters use multiple locations. Disrupting one location would not influence the availability of a service.

Environmental hazards The global spreading of datacenters raises some threats as already seen on confidentiality, but also on availability. Environmental hazards such as earthquakes and flooding affecting the security of data and economical hazards create possible security risks. For example recessions and inflation may decrease the providers quality of services and personnel [9]. When comparing this to traditional services, the location of the datacenter can be chosen. This decreases the vulnerability of the threat as the best location can be picked.

Weak recovery procedures Finally exploiting weak recovery procedures can be seen as a threat. When disaster recovery or business continuity processes are invocated inadequately, there might be a significant impact upon recovery time and thus availability [9, 30]. This is also the case in traditional systems.

3.3 Examples of security incidents

To illustrate the data security threats of cloud computing, we listed some example incidents that occurred in the past [9]:

- Availability - The Google organization had a disruption in its email service and was forced to apologize. In February 2009 its email service, known as Gmail, collapsed in Europe. Due to an update in the system data centers became overloaded. This overload had major impacts for the availability for the service. The service was unavailable for 2,5 hours.
- Confidentiality - In November 2007 a cloud services provider was targeted by a phishing attack. The phishing attack captured login credentials of an employee. The credentials were used to harvest confidential customer contact data. With this data attackers were able to send phishing emails with fake sales invoices to the organization's customers.
- Availability - In February 2008, a cloud storage service went down for almost four hours. This caused disruptions in several companies that were dependent on the cloud service. The cause of this availability issue was described as an unexpected spike in customer transactions.
- Integrity - In February 2011, Google's email service Gmail lost 150.000 email, folders and contacts. The cause of the disruption was a bug in an update on Google's storage platform. This bug deleted information of 0.08% of the Gmail-accounts. Google's backups on different physical locations were deleted too. To be able to restore the service, backup tapes had to be used. To repair the incident it took Google 4 days [35].

3.4 Mitigation of threats

In the previous sections we described the security threats that occur in public cloud computing. To minimize the security risks created by these threats, cloud providers try to decrease the vulnerabilities by implementing security measures. To validate if these security measures work as attended, audits such as SAS70 are conducted, compliance with legislation is guaranteed (e.g. Safe Harbor) and certifications such as ISO 27001 and CobiT are used [36, 37, 38, 39]. For more details about ISO 27001, SAS 70 and Safe Harbor, we refer to the appendices C, D and F. In the next sections we go into more detail about the mitigation of the threats put in place by cloud providers and compare them with the threats found earlier. We used the service offerings of large well-known public cloud providers as input for the comparison.

3.4.1 Confidentiality

Unauthorized inside users To decrease the vulnerability of access to data by unauthorized inside users, public cloud providers do extensive background checks before hiring staff. Based on the background of the employee and its function tight access control to data is applied. All actions done by developers and administrators are extensively logged and reported at multiple levels. Individual user sessions are identified and re-verified with each transaction.

Remote access exposure To decrease remote access exposure, public cloud providers harden host operating systems and implement firewalls on multiple levels [36, 38]. Use is made of intrusion detection sensors that log and report to a security event management systems. In some cases a third-party service provider continuously scans the network externally and alerts changes in baseline configuration.

Data leakage amongst other organizations At public cloud providers, isolation is used to prevent data leakage. This segregation of data and computing is done by implementing firewalls between instances.

Data location The unknown location of data in the original public cloud computing model is a large threat as it invokes legislation issues. To mitigate this threat, some public cloud providers provide the ability to choose the datacenter location at multiple geographic regions. In this way legislation issues can be mitigated.

3.4.2 Integrity

Data segregation As already stated in the previous section, public cloud providers use isolation to prevent data leakage. This segregation of data and computing is done by implementing firewalls between instances.

User access management Public cloud providers state that for each employee tight access control to data is applied. All actions done by developers and administrators are extensively logged and reported at multiple levels. Individual user sessions are identified and re-verified with each transaction. When changes in an employee's job function occur or an employee record is terminated, continued access must be explicitly approved to the resource or it will be automatically revoked.

Faulty infrastructure As faulty infrastructure is a result of improper configuration management, we looked for guarantees about configuration management in the product offerings. We noticed that public cloud providers use configuration management software and have ISO 27000 certified plans for changes in infrastructure. All hardware is monitored and audited by systems and network engineers. "Changes to infrastructure are authorized, logged, tested, approved, and documented in accordance with industry norms for similar systems" [36].

Secure deletion To decrease the vulnerabilities of data not being deleted, public cloud providers use standard deletion protocols. As stated in multiple market offerings: "Successful execution of a delete operation removes all references to the associated data item. All copies of the deleted data item are then garbage collected."

Limited monitoring possibilities As auditing datacenters is not possible in public cloud computing, cloud providers provide monitoring tools and use external parties to audit their services. Most common standards for audits that are conducted are SAS 70 (type 1 and 2), ISO 27000, and Safe Harbor. Third-party assessments that are conducted regularly are: Application & Network vulnerability threat assessments, penetration testing & code review and security control framework review & testing.

3.4.3 Availability

Change management Bad change management is a result of bad configuration management. As already described at the faulty infrastructure threat, we noticed that public cloud providers use configuration management software and have ISO 27000 certified plans for changes in infrastructure. All changes are monitored and audited by systems and network engineers. "Changes to infrastructure are authorized, logged, tested, approved, and documented in accordance with industry norms for similar systems" [36].

Denial of Service At public cloud providers, specialized hardware such as load balancers, packet filters, firewalls, and intrusion prevention devices, are in place to manage the DoS threat.

Physical disruption To prevent physical disruption threats, public cloud providers use redundant systems and physical security measures. Public cloud providers have multiple geographically distributed facilities, sharing space and utilities. Each facility is designed to run 24 x 7 and employs various redundant hardware to help protect operations from power failure, and network outages. On the physical security side, access to datacenters is limited to a small number of specialized personnel.

Environmental hazards To prevent environmental hazards such as flooding, public cloud facilities choose wisely for their geographical locations. To prevent disruption, redundant datacenters are used. In case of failure, automated processes move traffic away from the affected area towards other remaining sites. Finally cloud customers are able to choose on which location their services will be executed, this to prevent economical hazards such as recession and inflation.

Weak recovery procedures To prevent un-availability by weak recovery procedures, public cloud providers have documented and audited business continuity plans. In these plans redundancy and backup processes are described.

3.5 Concluding

In this chapter we answered the question: "What are the current top data security threats in public cloud computing and how are they mitigated?" By answering this question, we noticed that there are a lot of threats in public cloud computing. We chose to describe the 14 threats that were most referenced in literature as the top data security threats.

By analyzing the market offerings from well-known public cloud providers we noticed that for all of the threats measures are taken. To verify that the measures are taken and work as intended, public cloud providers have them audited (SAS 70) and certified (ISO27001 and Safe Harbor).

4 Data Security Requirements in the Dutch Financial Service Market

To ensure safe and secure IT services security requirements have to be set and managed. Security breaches at FS companies, e.g. breaches allowing unauthorized access to customer information, can be devastating. Events like this can be classified as operational risk, but these also expose the company to legal risk and reputational risk [40]. To prevent these security breaches, FS companies create security plans in which these requirements are included.

In this chapter of the thesis, we answer the question: What are the data security requirements in the Dutch financial service market? To answer this question, we searched for the data security requirements that have to be applied in the FS market to ensure that data is secure. In our search we found a lot of information about security requirements in FS companies all over the world:

- In [40], Vrancianu and Popa describe high level security requirements for E-banking services in Romania.
- In [41], important requirements concerning data security are described. E.g. appropriate application controls to ensure data accuracy, completeness, integrity, validity, authority and privacy.
- ENISA published a report that provides a decision model that bases the decision for cloud architecture on business & legal requirements and cloud computing threats for governmental clouds [22].
- In [42], requirements based on certifications such as ISO 27001 and SAS 70 are recommended.

In literature we found that the requirements for these services are derived from business requirements and obligatory regulations created by governments, international organizations and regulators to ensure that institutions keep data secure. This is underpinned by literature provided by the Cloud Security Alliance (CSA), see figure 9 [43]. As business requirements are service specific we chose not to mention them in this research.

With the knowledge that requirements are derived from obligatory regulations we extended our search and gathered information about a Dutch institution that assesses FS companies in the Dutch FS market called: De Nederlandsche Bank (DNB). De Nederlandsche Bank, translated: the Dutch Bank, is an organization which is responsible for safeguarding financial stability in the Netherlands. As our scope is about the Dutch FS market we use their information for the research.

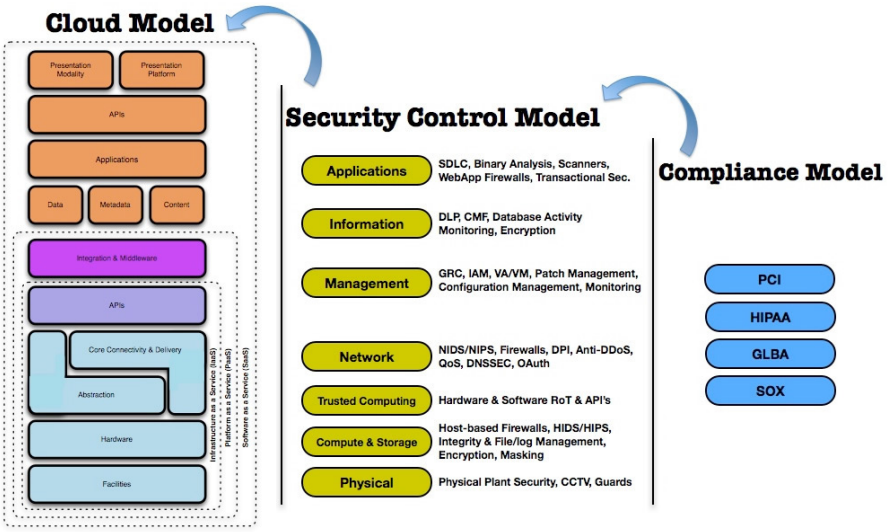

Figure 9: Deriving requirements for a cloud solution [43]

4.1 Requirements by The Dutch Bank

To ensure that Dutch financial institutions keep their information secure and their measures up to standard, the DNB provides an assessment framework to audit their organization. With this assessment framework the DNB tries to establish a quality standard to assess information security as objectively as possible. There are a lot of different audits and certification standards which all describe and benchmark financial service organizations. For example SAS 70, Basel II, Solvency II, etc. . This framework, specified on information security, is created by the CIA Working Group of the Netherlands Bankers' Association. The framework is based on the international standards: Control Objectives for Information and related Technology (CobiT) and ISO27002 [44]. As this framework has been especially designed for Dutch FS companies, we use this framework to derive the requirements.

The framework consists of a checklist to check maturity level of the required control measures. This checklist provides us indirectly with requirements needed in the FS market. The checklist is divided over multiple domains. The domains and their control measures are:

Strategy & Policies Information security requires management direction and support in accordance with business requirements, risks and relevant laws and regulations. To do this, the DNB provides several requirements in this domain, starting with an information security plan. To provide direction and support for information security in accordance with business, risks and compliance requirements, a security plan has to be created. To ensure reliable and secured

information to support business processes and to seamlessly integrate applications into business processes, an information architecture has to be developed. Another requirement in this domain is: determine technological direction. This means that companies should provide stable, effective and secure technological solutions enterprise wide to enable timely response to business requirements and changes in law and regulations, industry and technology developments. Finally IT risks have to be assessed and managed. This to ensure that information security risks are discovered, prioritized and are accepted in a timely and structured manner aligned with the enterprise's appetite for IT risk and the organization's risk management framework.

Organization Information security has to be managed within the organization through an embedded structure and a set of roles and responsibilities. The requirements on this domain are: Information Security must be managed at the highest appropriate organizational level, so the management of security actions is in line with business, risk and compliance requirements. Data and system ownership must be established to provide accountability and ensure that data integrity, confidentiality and availability are in line with business and compliance requirements. Finally a segregation of roles and responsibilities must be implemented to reduce the possibility for an individual to compromise a critical process.

People In this domain requirements to ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities are listed. To ensure this, management of IT human resources is needed. This means that functions are staffed properly with reliable and skilled people.

The DNB also describes that people should have the knowledge and skills to allow effective and efficient operations of new or adjusted technology in line with the security policies and procedures.

Processes In the process domain requirements are listed to ensure that system and infrastructure development, maintenance and access is performed in a secured way and that they comply to the information policies, standards and procedures, and laws and regulations. To ensure this, all changes, including patches, support enterprise objectives and must be carried out in a secure manner. This has to be done in a way that it does not disrupt day to day business. On the continuity management side, the DNB describes that counteract measures have to be taken to prevent interruption of information systems. Another requirement in the processes domain is management of data. An FS company has to maintain the completeness, accuracy, availability and protection of data. Configuration Management has to be on maturity level 3 also, this to ensure that all configuration items are appropriately secured and security risks minimized by ensuring the enterprise's awareness of its IT-related assets and licenses. Third parties (suppliers, vendors and partners) services have to meet business

requirements so that related business and IT risks associated with continuity and security are minimized. To avoid breaches of any law, statutory, regulatory or contractual obligations, monitoring has to be applied. Finally User Account Management has to be implemented. This has to be done to ensure that all users only have authorized access to data and functionalities, and their activities within the IT environment are uniquely identifiable.

Technology In the technology domain, requirements to ensure the protection of information in networks, the supporting infrastructure and the secure exchange of information are provided. The first requirement in this domain is secure infrastructure. Which means that security techniques and related management such as firewalls, security appliances, network segmentation, intrusion detection, trusted path or medium, encryption) are used to secure data storage and transport within the enterprise's technical infrastructure, flows from and to the network and mobile devices. The applied techniques should be in accordance with the related impact consequence or data classification. To ensure protection on technology malware attack management should be in place. This means preventive, detective and corrective measures such as security patches and virus control are in place and up-to-date. The final requirement given by the DNB is that infrastructure components are protected. This means that the technology is hardened, security-related technology is made resistant to tampering, and security documentation is not disclosed unnecessarily.

Facilities The final domain of the framework is facilities. In this domain physical security is addressed. It is required that physical security measures such as fire prevention, vandalism, etc. and physical access management are defined and implemented to secure facilities.

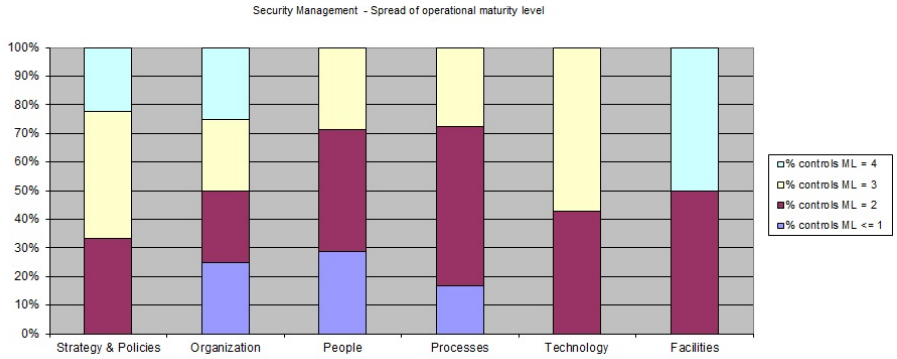

Figure 10: Graphical Overview Maturity Levels DNB Assessment [44]

The DNB provides a spreadsheet that automatically creates graphs (see figure 10) and indicates the state of each control measure. In the assessment

framework a measure is in control when is has a maturity level of at least "3" [44]. Widely recognized technical standards to secure customer data (e.g., ISO 27001), may not always match perfectly to national requirements for appropriate measures [22]. For this reason the next section we will describe the national requirements directed by the Dutch law.

4.2 Legislation & Compliance

In the Netherlands, FS companies have to apply to the obligatory regulations in their business. These regulations consist of legislation in the Netherlands itself, but also some regulations required by the European Commission (EC) [45]. In the next paragraphs we will explain the regulations which are relevant for security of personal data in cloud computing.

4.2.1 Personal Data Protection Act

The first law applicable to the FS market required by the EC is known as: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [46]. The main purpose of this law is to harmonize the privacy laws from the different member states of the European Union (EU) and to provide a basic standard on privacy protection [45]. As the Netherlands are part of the EU, this law is also applicable for the Dutch FS market. The specific Dutch data protection law is derived from the EC law and added some member state specific information such as monitoring commissions and sanctions. During this thesis we will refer to this law as the Personal data protection act. The main article of this act is:

> "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data"

To understand this law, the EC gave definitions for multiple parts of the act, we provide you with the relevant ones for this phrase of the act. The EC defines personal data as any information relating to an identified or identifiable natural person. With processing of data the EC means any operation performed upon personal data.

The act makes a distinction between data controllers and data processors. A data controller is a legal entity that chooses how data is processed is responsible for compliance. If a data controller chooses to use a third party (a data processor) for the data processing it should ensure that the processing is done in compliance with the EU directive. If the data processor is located in the EU, and the data controller doesn't, the data processor must comply with the EU Directive [45].

In the next paragraphs we will only highlight the phrases of the act which are relevant for this research. The EC describes two situations in which this act doesn't have to be applied namely, when an activity falls outside the scope of

the Community act, such as operations concerning public security, defense and state security. The second situation is that the act shall not be applied by a natural person in the course of a purely personal or household activity. Some interesting phrases in the act applicable to cloud computing are: In article 6 of the act, the EC describes that the data shall not be kept longer than necessary for the purposes for the data were collected or processed.

Data may only be processed when the data subject has given his consent, when processing is necessary for compliance with legal obligations, and to protect the vital interests of the data subject [22].

The data controller must implement appropriate technical and organizational measures appropriate to the risk to protect personal data against accidental or unlawful processing of data [22].

The act also describes that when the data is processed outside EU borders, the national law of the other country or the safe harbor agreement has to be applied. The safe harbor agreement is an agreement between the US and the EU. The agreement aims to align the process for US companies to comply with the EU Directive [45, 22, 47].

In the act a distinction is made between transfer of personal Data to third countries and member states of the EC. Sensitive data processing in third countries may only take place when there is compliance with the national provisions and the provisions of the EC personal data protection act, which means that the third country ensures an adequate level of protection. The data controller is responsible to monitor the processor [46, 22].

4.2.2 Privacy and Electronic Communication Act

The second act applicable to cloud computing in the Dutch FS market is: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. As this is a very long name, we chose to use the name: Privacy and electronic communication act. As the Netherlands apply this act, we directly use the EC act as information source for this paragraph [48]. Directly quoted from the act:

> This directive provides for the harmonization of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

In article 3 of this act, the EC describes that this act is applicable to the processing of personal data in connection with the provision of publicly available electronic communications services in public networks, including public communications networks supporting data collection and identification devices. This

gives us the information that this act is also applicable to public cloud computing as it provides services that support data collection. In the next paragraphs we will highlight the relevant parts of this act for this research.

The provider of a publicly available electronic communications service has to take appropriate technical and organizational measures to safeguard security of its services. In regard to the state of the art and the cost of the security measure implementation, the measure shall ensure a level of security appropriate to the risk. Amended to the 2002 version of this act these measures should:

- ensure that personal data can be accessed only by authorized personnel for legally authorized purposes;
- protect personal data stored or transmitted against accidental or unlawful processing, access or disclosure;
- ensure the implementation of a security policy with respect to the processing of personal data;

National authorities must be able to audit these measures.

Finally the act also obligates that "traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication." [48]

4.2.3 Financial Supervision Act

To monitor the Dutch financial service sector, a Dutch law called "Wet op het financieel toezicht" is applied [49]. Translated this act is called the Financial supervision law. This law is applied to create a transparent, target oriented and market oriented FS companies. The main cause of this act is to give monitoring institutions rights to obtain information about FSs administration.

In this act, there is no direct article that relates to specific data security. As this act demands transparency to monitor FS administrations, it indirectly directs some security requirements. Because FS companies are monitored their administration has to be complete and right. In order to guarantee this their security must be at appropriate level. If a FS company doesn't have the right security measures, they can never guarantee that their administration is correct. This leads to the indirect requirement that the integrity of the data must be secured.

4.3 Concluding

In this chapter we answered the question: "What are the data security requirements for IT services in the Dutch financial service market?" To answer this question we referenced literature about requirements at financial services companies. As we could not find literature that described the requirements specifically related to Dutch FSs, we used a framework of the CSA (see figure 9) to gather the Dutch requirements ourselves.

We discovered that the data security requirements in the Dutch FS market were a combination of legislation and security standards demanded by a financial regulator, the DNB. The standards that are demanded are the ISO27000 series and the Cobit 4.1 standard. These standards are common standards in security management. Looking at the differences between Dutch and global requirements, we see that legislation is distinctive.

We discovered that there are three acts in legislation that cover data security in Dutch FSs. The acts found do have some overlap, but their main demands are that data containing sensitive (personal or transactional) information should be stored "adequately" and security management must be transparent and auditable by national authorities and regulators.

5 Public cloud computing in the Dutch financial service market

In this chapter of the thesis we answer the third sub question of the research. The sub question is "To what extent is cloud computing used in the Dutch financial service market?"

To describe the current usage of public cloud computing in the FS sector, we did an explorative survey and we interviewed different FS companies about the use of public cloud services. Because the FS sector has a large number of different companies with different products and services (e.g. insurance, loans, etc.) we grouped the multiple company types to create clarity. Based on this classification we describe the current state of public cloud computing at Dutch FS companies.

5.1 Explorative Survey

To get some orientation in this research field of cloud computing, we did a quick scan by means of a survey at the Landelijk Architectuur Congres (LAC) 2010. The LAC is a congress where architects meet and share information. Questioning these architects would give us answers to get some orientation. We chose for architects because they should be people with knowledge about cloud computing and the use of it in their company. The questions we asked were mainly about the use of cloud computing in their company and the reasons for it. We also asked questions about the security of their services.

Of the 400 architects that were present at the congress, we questioned 46 architects. However, only 4 of these architects were active in the FS market. To use the answers of the survey we chose to draw conclusions on all the answers. The conclusions of this survey provided us with insights about the cloud computing opinions of architects active in different sectors such as, public, finance, IT, Healthcare and Retail. These findings are that these architects:

- use both private (or hybrid) and public cloud computing. (Except the public and finance sector)
- SaaS solutions are mostly used.
- believe that cost aspects, flexibility and scalability are the main reasons for choosing cloud solutions.
- do not use cloud computing because: it is too new, they don't want to lose control and security is lacking.
- believe that integrity and confidentiality are the main security issues in cloud services.
- believe that their own datacenter is more secure than the datacenter of cloud providers.

For the complete survey we refer to appendix A in this document.

Some of the findings of this quick scan are underpinned by KPMG. KPMG did a survey based on the views of 125 decision makers and business managers in the Netherlands, to conclude that cloud computing is more than just hype. This survey states that industrial market sectors already adopted cloud computing services on a large scale (over 50 percent). But there is a significant difference when looking at the figures of financial services and the public sector. In the financial services sector only 32 percent is using cloud computing services. For the public sector this is 33 percent [13]. Some other similarities found were that:

- SaaS solutions were mostly used.
- Flexibility, scalability and cost savings were main reasons for choosing cloud solutions.
- Security issues were main concerns regarding the use of cloud computing.

5.2 Financial Services

In the Netherlands there are a lot of different financial service companies. E.g. Financial service providers, Money transaction offices, Investment institutions, Insurers, etc. All the financial services operating in the Netherlands are kept in an updated register at the DNB. Their list, classified on permits and legislation, is used as input for the classifications made in this section. In this register, the Dutch Bank distinguishes between 13 groups of financial services [50].

A further classification of these 13 groups into 3 groups can be made as shown in figure 11. This leads to the classification of the Dutch FS market, as follows:

- Banks - Important Dutch companies in this group are ABN AMRO, ING Bank and Rabobank.
- Insurance companies - Important Dutch companies in this group are Nationale-Nederlanden, Aegon, Achmea, PGGM and ABP.
- Capital Markets - Important Dutch companies in this group are Rabobank, ABN AMRO and ING Group.

As stated earlier, there are a lot of financial services types which all have their own specific requirements. To maintain a reasonable size and scope for this research, we chose to pick two groups to continue the research. The chosen groups are banks and insurance companies. In the next sections we provide information about the current state of public cloud computing at banks and insurance companies.

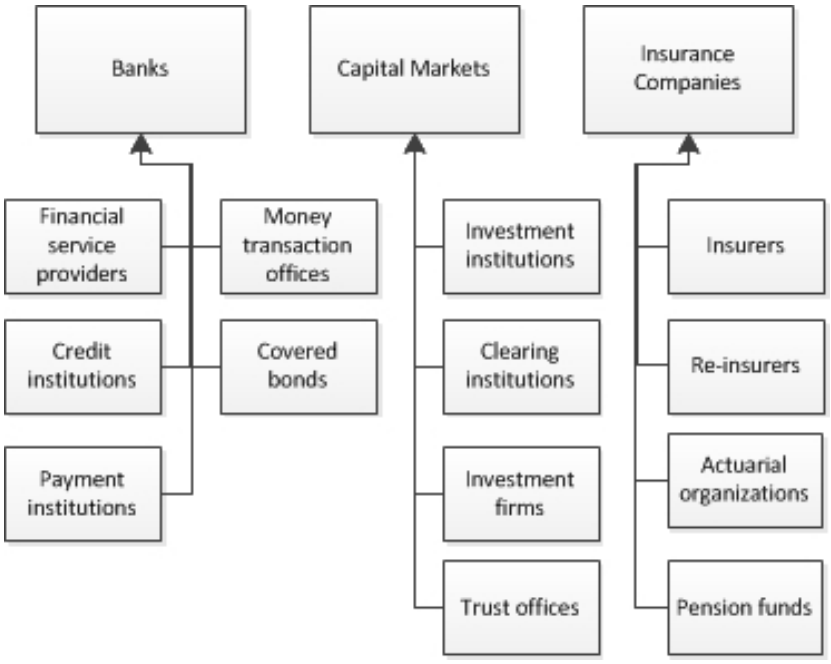

Figure 11: Grouping process

5.3 Interview Rationale

The interviews we conducted were all structured interviews on the basis of 20 interview questions and an interview approach & methodology as described in Appendix G. The objectives of the interviews were to:

- define current usage of public cloud computing services in FS companies;
- define security reasons for (not) implementing cloud computing services in FS companies;
- enable contact for validation of findings;

The validated findings and our conclusions based on them are described in the following sections of this chapter.

5.4 Public Cloud Computing at Banks

We interviewed two experienced security experts at two major banks in the Netherlands to get a clear view about the current state of cloud computing at banks. To keep the two banks separate but anonymous, we use the names Bank A and B.

5.4.1 Bank A

Profile Bank A is one of the largest banks in the Netherlands. Bank A has 30.000+ employees that are active at 1.000+ locations in the Netherlands and is internationally active in about 50 countries. Bank A is a conservative bank that is researching possible uses of Cloud Computing for their services. At this moment main public cloud computing subjects are research subjects about risk management and responsibility of cloud providers. At Bank A we interviewed a security officer who has 4 years of experience in this function.

Public Cloud Computing Usage At the moment of interviewing Bank A uses public SaaS and PaaS non-core services. During the interview we noticed a kind of carefulness on the implementation of public cloud computing. There were only a couple of public cloud services that were used and they were only in production for about one year.

We asked the security officer why they implemented public cloud computing. The main reasons for Bank A to switch to and implement public cloud services were:

- Cost savings
- Flexibility
- Scalability

The usage of public cloud services at Bank A is chosen based on low security classifications. For example the SaaS services at Bank A were used to provide non-critical supporting services.

The PaaS services at Bank A were used to do tests on a very small scale and with non-critical data. The reasons for keeping the test at small scale and the usage of non-critical data is because security breaches in testing environments might disclose new trends or possible defects. These issues, even when a system is not in production can raise reputation damage.

Bank A told us that for many security and legislation reasons they do not use public cloud computing in core services. Regulation combined with the data location threats is one of the issues that make the implementation of these services a hard job. For example the case where at one location data is legal and in another location the same data may be illegal, see section 4.2.1.

A shortlist of the reasons for not switching to public cloud computing given by Bank A was:

- Data location is unknown. This arises regulatory & legislative issues. For example: Location restrictions as obliged in the Personal Data Protection Act(section 4.2.1)
- Lack of control
- Cloud providers deliver low software quality in contrast to own software or software delivered directly to the organization.
- Security requirements at banks are far stricter than the services that are offered by public clouds.

Data Security Risks To get more information about data security risks in the FS sector, we asked Bank A about their view on the risks of information security in public cloud computing.

Bank A states that the major risks in public cloud computing for their organization are mostly based on confidentiality and integrity issues.

Bank A states that availability threats in public cloud computing have a lesser occurrence and thus their risks are addressed differently. They can become high security risks when the cloud layers are placed at different (small) cloud providers. When this is the case, different parties have different responsibilities in which extra issues can occur.

Security breaches for banks have major impacts for reputation. Minor incidents (that occur once or twice) are repairable and taking repair actions may even create a reputation increase for banks. Structural security breaches (which are the case in public cloud computing) are not repairable and damage reputation.

To mitigate and manage risks, Bank A executes existing risk management processes as implemented in the bank. In this process additional attention is given to security testing, as well as to contract clauses concerning liability and vulnerability disclosure obligations. System requirements are tested by penetration tests and ethical hacking tests. Also ISO 27000 (see appendix C) and the DNB framework are used to assess the services.

Data Security Classification Bank A assigns security classifications to all of their systems. The data security classification used is based on CIA requirements. The classifications made are based on the magnitude of the risks related to the system. For example: Personal identification data has a high confidentiality risks and e-banking data has a high integrity risks. For more information about this classification we refer to appendix H.

To be able to use them, Bank A translates data security classifications into system security classifications for a specific service. In Bank A, three point scales are used to classify services. For each item; confidentiality, integrity and availability a value of low, medium or high is given. A higher classification means

that the related risks have more impact. On the requirements side this means that services with high levels need more compliance on security requirements.

Summary From the answers retrieved during the interview we summarize that at Bank A only two public cloud services are used. These services are used because of cost savings, flexibility and scalability. Both of the services (SaaS and PaaS) do not use sensitive or personal data. Only data relevant for non-critical processes, e.g. system testing, is included.

The reason for not using critical processes stated by Bank A is: Implementing public cloud computing is decreasing costs but increasing risks. Banks have a strong security task. When security breaches occur, reputation damage will have major impact.

The cost benefits of moving to cloud computing are not enough for banks to accept the risks associated currently with cloud computing.

At bank A services are classified by means of a CIA classification. With this classification Bank A is able to select services that can or can't be placed into the public cloud.

5.4.2 Bank B

Profile Bank B is like Bank A one of the largest banks in the Netherlands. Bank B has 30.000+ employees that are active at 500+ locations in the Netherlands and is internationally active in about 50 countries. Bank B is researching the opportunities of cloud computing, but not on the public cloud computing deployment model. In Bank B we interviewed a Chief Architect responsible for IT Risk and Security. The interviewee had 20 years of experience and is fulfilling this function for about 1,5 years. He experiences cloud as a next step in the evolution of sourcing models. "It is hyped as something new, but it isn't. It is just shifting responsibilities."

In the interview we asked what percentage of services would gain benefits from elastic computing and storage power. The interviewee responded that at this moment the average load on their servers is 4 to 8%. When using virtualization, such as used in cloud computing, estimates are that this can be scaled up to 70-80%. This means fewer machines, less management while keeping the same capacity.

At the moment Bank B is working on a business case in which virtualization reduces the number of 17 datacenters to 2. The research for a clear case is very hard because there are a lot of parameters that create lots of uncertainty. To give an example, a question in this research is: is it good for Bank B to only have 2 datacenters. The research becomes even harder because there are not enough reference cases to give examples of situations that proof that the virtualized setup is working as intended.

Public Cloud Computing Usage When asking Bank B if they were using public cloud computing for their own services, the first answer that was given was: "Hell no!" When asking them to go more into detail, Bank B stated that

they do not use any public cloud service for internal services. There are even policies that prohibit employees to use public cloud applications such as Google Docs and Dropbox to store sensitive data. Nevertheless, for e-learning and online training solutions, Bank B does use services that might be public SaaS services.

The main reason to do research about implementing public cloud computing for Bank B is cost reduction. We asked about the flexibility and scalability benefits of cloud computing. The answer we got was that they had 70+ datacenters which already provided the flexibility and scalability needed.

The main reasons for Bank B to not use public cloud services for internal processes are:

- Legislation prevents the usage of public cloud. For example: Location restrictions as obliged in the Personal Data Protection Act(section 4.2.1)
- Not feeling safe when data is stored between the data of others.
- The perception of the Enterprise: Outside the perimeter you can trust none.
- Hard to couple internal processes to external cloud services. (Application and identity integration)

When asking about shifting risks, Bank B answered that this is not the case as they have a much higher responsibility to their clients than cloud computing providers have towards them.

An interesting finding we got during the interview was a statement of the expert: "Purely based on security in public cloud computing services, risks are lower than at on-premise services." Nevertheless, Bank B doesn't move to the public cloud because of the perception of the enterprise and their customers; "We don't want to lose trust". If a bank loses trust it can go bankrupt in a couple of days. An example of such a situation happened in The Netherlands in October 2009. A bank run was executed on the DSB bank and after a couple of days the bank was declared bankrupt [51].

When bank B publishes that they are moving to an Amazon cloud, someone may stand up and publish that sensitive data is stored next to their iTunes library. This will cause changes in the perception of security customers have about a bank. Changes in perceptions might result in reputation and trust damage which can cause a bank to go bankrupt.

Data Security Risks When looking at the lower levels of cloud computing such as IaaS, Bank B doesn't see a difference between the security at traditional datacenters and clouds. They state that the main security risks are on the communication line. At higher levels such as SaaS services, they do see a difference, because the control is left over to the cloud provider instead of themselves. Before moving to public cloud computing, Bank B states that the security policies

at the cloud provider must be better or similar to the minimal standards (policies) at the bank. To check the compliance to the security policies, Bank B uses the standards CobiT 4 and ISO27001. They also look very careful at SAS70 Type I and II statements of external auditors.

Bank B uses a set of minimal standards for their security requirements which are derived from ISO and CobiT standards. Every service gets its own set of requirements. Due to this it is impossible to define a standard based on CIA for all of the services. When asking them about the DNB security framework they stated that their checks were better than the ones from the DNB. As Bank B uses the ISO and CobiT standards and the DNB framework is derived from them, Bank B is compliant to the DNB framework.

Data Security Classification Bank B uses data security classifications to differentiate between sensitivity of data and services. The model used is the CIA classification model (see appendix H). On every aspect of the triad (see section 3.1) 4 levels are used to classify the data. With this classification Bank B is able to select services that can be placed in the public cloud. When asking what rating would be the threshold of putting services in the cloud, Bank B responded with CIA 2,2,2.

Summary Bank B states that public cloud computing is a step too far for banks. They have more trust in community, joint venture or private clouds. Having core data stored in datacenters next to the photos of Aunt Anny is not what Bank B wants. Another reason of not using public cloud computing is that banks need the right to audit their services. This is obliged by legislation, see section 4.2.2 and 4.2.3. In public cloud computing this is not possible. Finally the connection between the internal network and the public cloud comes with several security risks which cannot be accepted.

Bank B is researching the possibilities of public cloud computing because of the cost saving benefits. Flexibility and scalability are no benefits compared to the datacenter capabilities they already have. Nevertheless, cost savings are not core business for Bank B. Trust, security, and client perceptions are the main goals which may cost money.

Before implementing public cloud services, Bank B does a major risk analysis. A service is held against a large number of requirements. Most of these requirements are derived from standards such as ISO 27000 series and CobiT.

5.4.3 Cases

During the interviews we proposed several core services of banks and asked why they could or couldn't be placed in the cloud. To select the core the processes that banks have, we use a model created by SAP called Business maps. For different types of businesses, SAP created solution maps to describe which of their solutions are applicable for specific business processes [52].

In the banking solution map SAP describes the different parallel processes that are used in a bank. The solution map is depicted in figure 12. The map

uses different operation types. Because the research is about data security requirements in FS services, we chose to select three specific operation types that use different types of data to analyze their services. The business groups selected are: Product Management, Sales & Service, and Cash and Liquidity Management [52].

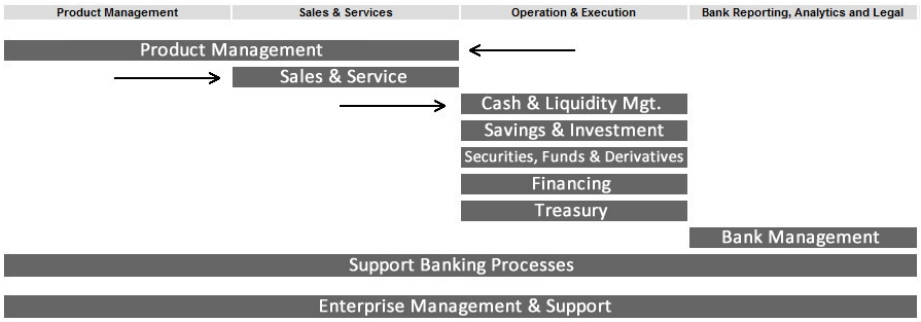

Figure 12: SAP Solution Map - Bank [52]

Product Management Product Management is about developing strategies that will increase product demand over the product's life cycle. These services help to streamline the implementation of new products, to reduce costs by configuring the products in a certain way, and to test product performance at an early stage. Data stored and used in these services contain product and customer information.

When asking both banks about the implementation of product management into the public cloud we got the answer: Product management services cannot be placed in the public cloud because data in these services has a too high CIA rating which exceeds the threshold rating of the public cloud. Examples of sensitive data used in this type of services are:

- Client administration data containing personal data.
- Agreement administration containing data that when it gets modified affects large groups of customers.
- Product administration containing data that when it gets modified affects large groups of customers.

Sales and Service Sales Management services in a bank are used to streamline customer interactions, and to provide integration of front end processes with back end processes. In these services CRM data is used to provide banks with insights into business operations for marketing and sales. An example service that can be provided with these insights is personalized contact, advice and services for the customer. The data used in these services contain personal data of customers.

When proposing the Sales and Service services, the experts separate them into two separate parts, one part contains services before a person is a customer and the second part is when a person is a customer. The difference lies into the fact that once a person is a customer, the bank is responsible for that person. In the stage before people are customers, public SaaS solutions can be used to support them. Once they are customers the impact and thus risks rise. Banks don't want the high risk sensitive information to be stored in the public cloud, this because of security risks and legislation about personal data.

Cash and Liquidity Management Cash and Liquidity Management services cover all the services that are linked to cash-based or cash-near transactions a bank offers to its customers. Services in this group support scenarios such as: management of current accounts, card management, and payment operations. Data used by these services contain personal data of customers and critical transaction data.

When we asked if Cash and liquidity management services could be placed in the public cloud. Bank A told us that when doing this, special care should be given to the integrity issues as these have large impact on transaction and e-banking services. The answer Bank B gave was: "hell no". This because the data used in these services contained too much sensitive data in which integrity issues cannot be accepted. Bank B did see opportunities in Community clouds with other banks that have the same security requirements and responsibilities about the data.

5.5 Public Cloud Computing at Insurance Companies

To describe the state of cloud computing at insurance companies, we interviewed IT security experts at two well-known Dutch insurance companies to gather information about the current state.

5.5.1 Insurance Company A

Profile Insurance Company (IC) A is market leader in insurances in the Netherlands. IC A has 20.000+ employees that are active at 20 locations in the Netherlands and is internationally active in 10 countries. At this moment IC A is doing research about how to implement and develop cloud services. The first services that would be placed in the cloud will become the services that support processes applicable to customers and do not contain sensitive data.

IC A is also researching and developing another business case for services that do contain sensitive data. The research is concentrated at the security of sensitive data with high impacts. Once this research is done and the outcome is positive, actions will be taken to put services with this data into the public cloud.

IC A is restrained in moving to public cloud computing. It does not have policies that urge them to speed-up cloud implementations. Nevertheless, the security expert told us that about 80% of their services would probably gain

benefits of the elastic properties of public cloud computing. In some cases, costs could be decreased up to 200 times and cloud services' availability would even be increased. The huge cost difference was partly explained by the dedicated hardware needed for traditional systems such as AS400 that need their own (not commodity) hardware.

Cloud Computing Usage At the moment of interviewing, IC A has one public SaaS website in production. This service is up for about one month and provides a website. The service does not contain sensitive information and has the assurance that the data does not leave the EU. The adopted SaaS service is not running core applications as the interviewee stated:

> We do not use the public cloud for any of our core services.

For e-learning situations Insurance Company A also uses services that might be public SaaS services. In these services no data of the company is used and the organization is a customer of the service.

When asking the security officer the main reasons for switching to public cloud computing for IC A, he directly answered: "money". Cost reduction was the most important factor for IC A to move to cloud solutions. On the second and third place came scalability and flexibility.

We asked if shifting risks to cloud providers could be a reason. This was not the case because IC A feels responsible for everything they do. When choosing a cloud provider they make agreements about how they can use active monitoring to ensure security for which they feel responsible.

The reason for not switching to public cloud computing for IC A is because of the security risks. Their reaction:

> There are not enough guarantees on the security aspects.

Breaches in security cannot be accepted, they cost money and decrease reputation.

Data Security Risks To be able to visualize all risks applicable to a service, every sourcing partner is held against sourcing requirements. These checks (ISO 27000, SAS70, ISF maturity check) provide information about the maturity of the provider and if the provider is in control. As the Information Security Forum is a closed organization, we could not access documents describing the ISF maturity check. By asking what kind of check this was, IC A responded that is was a security check like the ISO 27000 and CobiT checks, but specified on cloud computing.

From these checks IC A notices that there are two types of public cloud providers:

- New immature cloud providers that have security measures in place, but don't know how to react at security breaches. New providers often use other cloud providers for their infrastructure. This increases risks such as unknown data location and who has (physical) access to the data.

- Mature providers such as Amazon know what to do in security breach situations, are able to provide economies of scale and can assure that the data does not cross borders (e.g. EU).

IC A stated that they will certainly not use new immature cloud providers for their services. At this moment no sensitive data is placed in the cloud to reduce risks. To become able to place sensitive data in the cloud extra measures such as encryption techniques are being researched at this moment.

According to IC A, confidentiality and integrity risks are lower at their own traditional data centers. On availability security risks, traditional services cannot compete with cloud services. Availability is much better in cloud services.

Data Security Classification In IC A two different data classifications are made. One classification is based on Dutch legislation called: Wet Bescherming Persoonsgegevens (see section 4.2.1). And the second classification is based on an information classification framework provided by the ISF. IC responded that this framework is similar to the CIA framework as it classifies data on CIA requirements and impacts.

At this moment IC A uses a threshold similar to the CIA threshold of 1, 1, 1 for data that can be placed in the public cloud. Data with a higher rating is not yet determined.

To check the requirements set at the classifications for their services, IC A uses the ISF standard of good practice. This standard is a checklist which addresses topics that are key to security and risk management strategies, including: policy, outsourcing, privacy, intrusion prevention, wireless communications, mobile computing, and computer forensics. Using this standard is part of their sourcing strategy which is applied to every sourcing provider.

Most of the checks are done by themselves, but IC A also bases the checks on the reports of external parties such as auditors and accountants.

Summary With the answers retrieved during the interview we conclude that at IC A only a few public cloud services are used. In these services no sensitive or high risk data is used. The services that are running in the public cloud are services that do not contain core processes.

IC A is doing risk management research about possible public cloud solutions. This is because public cloud computing has major benefits such as cost reduction, scalability, flexibility and the increase of availability.

The reason that there are only a few services implemented is because the lack of guarantees on security risks that public cloud computing brings in contrast to the traditional systems.

We noticed that IC A in the FS market is very careful when moving control to third parties. Trust in these third parties is very important. Another aspect that is very important is reputation. At FS companies, damage to this can occur in a split second. For this reason IC A is very careful with implementation of public cloud services.

5.5.2 Insurance Company B

Profile IC B is a well-known insurance company in the Netherlands. IC B has 6.000+ employees and has over 5 million customers. To get practical information about the use of public cloud computing at IC B we interviewed an Information Analyst with 13 years of experience. His personal experiences on cloud computing are: the use of Google Docs and Mail.

When asking about the experiences he got with cloud computing in the business perspective. He told us that he:

- worked on a project group that implemented a public SaaS CRM service;
- did research about possible SharePoint implementations in the cloud ;
- worked on an implementation of grid computing for large computing batches;

At the moment of speaking most of the services at the IC are still running on traditional on-premise datacenters. When asking what percentage of services would gain benefits from elastic computing and storage power, the interviewee responded that approximately 60 - 70% of the current services offered could gain benefit from elastic characteristics.

When we asked about the cost savings, a direct answer could not be given. In their model, costs made in the datacenter are directly calculated to the business unit that uses the service. This is a different calculation than the calculations used in cloud computing. E.g. pay by CPU cycles used.

When we asked if they could give us an estimate about the cost savings, a factor 4 in cost savings was expected. This was underpinned by a business case specialized on a public SharePoint service implementation. The main reason for cost savings in this business case was the absence of hardware for backup and redundancy.

Cloud Computing Usage IC B uses several cloud services. Most of them are private services such as a private SharePoint service, a private policy administration service and an infrastructure as a service for calculating large batches.

One year ago, IC B implemented a public SaaS CRM service. This service is located at a public cloud provided by Salesforce.com. The CRM service is used for sales processes with their possible customers. Once the possible customers become clients with a contract, internal services take over.

The reasons for implementing the public service for IC B are:

- The SaaS product itself, perfectly fitted to the organization;
- Time to market;
- Cost reduction: pay per user license;
- Scalable per user;
- Loss of maintenance (costs);

Because this is only one service that is running in the public cloud we also asked why other core services were not in already placed in the cloud. The main reasons for not switching to public cloud computing stated by IC B were:

- Keeping control over their own services;
- Unable or very hard to change services in order to comply with Dutch legislation;
- Unable or very hard to change services in order to compete with other insurance companies;
- Unknown data location;
- Data ownership: who can change my data? How can I get my data back?;

Data Security Risks IC B takes the security risks in public cloud computing into account. Before a service is placed in the public cloud, several checks, audits (SAS70) and certifications (ISO 27001 and Safe Harbor) are referenced before using a public cloud service.

To prevent security breaches, IC B holds every service against a list of security requirements. In this security risk assessment a CIA rating is used to classify the service and the used data. Based on this classification several security measures are addressed. Some examples of measure given were: encryption techniques, access and identity management is not outsourced, and no use of mobile devices.

IC B uses: ISO 27001 certification, SAS 70 statements, External audits (based on legislation) and site visits to check if the service provider complies with the demanded requirements.

Data Security Classification As already described IC B uses the CIA rating framework to classify data. Based on this classification requirements for security measures are demanded. When asking what CIA level would be the threshold of placing services in the public cloud, IC B stated that they used rating: 3,2,2.

Summary IC B is an IC that is already using public cloud services for some core processes. The services used at this moment contain future customer data, once customers sign a contract, the information is passed to internal traditional services. In this way they prevent that sensitive data on which they are responsible is placed in the cloud.

The reasons for using the public SaaS CRM service at IC B are: the product perfectly fits into the organization, time to market speed increases, Cost reduction, scalability per user, and the loss of maintenance (and thus costs).

Not all of the processes at the company are placed into the public cloud, the main reasons for this are: keeping control and ownership, legislation, unable to change services to own specifications, and unknown data location.

Before services are placed into the cloud, risk management is executed. IC B uses certification and audits to check if cloud providers' policies comply with their own policies.

5.5.3 Cases

Finally we proposed three core insurance services and asked the experts to describe if they could be or were already implemented in the public cloud. To select the services we used the Insurance Solution Map from SAP. In this map, SAP describes the different parallel processes that are used in an IC. The insurance solution map is depicted in figure 13. As in the banking section, we chose to select three specific operation types to analyze their services. The business groups selected are: Sales, Policy Administration, and Claims [52].

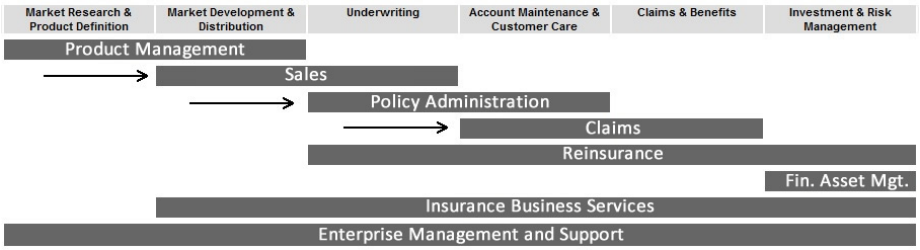

Figure 13: SAP Solution Map - Insurance [52]

Sales Sales services support the relation between the customer and the insurance company. With these services, products are offered to customers. Data stored in these services contain information about the insurance policies and customers.

At IC B, a part of the sales services is already implemented into the public cloud. This differs with IC A that does not use any public cloud services yet. We say yet, because this is a service that IC A would place in the public cloud at first. The reason for this is that the data in services such as product offering services does not directly contain any sensitive data for the IC.

Policy Administration Policy administration services cover the processes from capturing signed applications up to the issuing or rejection of it. This means that these services do checks, risk assessments and premium/benefits calculations according to product requirements. At the end of the process a new policy is issued or rejected. Data stored in these services contain personal data of customers and transaction data.

When looking at the Premium/benefits calculation services for at Policy Administration, Insurance Company B stated that they used private cloud services for this. Their average CIA rating for these services was rated at 2,2,2. The

reason of not placing this service in a public cloud was that there were no public SaaS solutions available for this type of service. When this service would become available, serious research will be done to check if this service can have benefits for the company. One side note had to be taken, these services had to be located inside the EU for legislation reasons. IC A was somewhat more careful, they did understand the benefits of calculating in the cloud, but they didn't want to place the core transaction systems that are part of the policy administration service into the public cloud.

Claims Claims handling is the business process executed by insurance companies which serves customers (policy holders) that claim to have experienced a loss for which they have an insurance policy with the company. Services in this group provide processes that evaluate claims, settle claims, and detect fraud. Data stored in these services contain personal data of customers and transaction data.

During the interviews we noticed that services to support the settlement of claims are not yet placed into the cloud. IC B states that this is because there is no service available for this yet. When looking at service that settle claims in insurance company A, they state that interaction with the client might be placed in the cloud. But this is unsure as these services use more sensitive data and research has to be done first. The calculations that are done with the data cannot be placed into the cloud as these have too high CIA ratings.

5.6 Summary and Discussion

In this chapter we gathered information to answer the question: "To what extent is cloud computing used in the Dutch financial service market?" In the following bullet lists we summarize the gathered information.

The public cloud services that are used in the FS companies are services that:

- Take benefits from the cost savings by economies of scale, management, and pay-per-use.
- Take benefits from the flexibility, scalability and time to market speed.
- Do not contain data that might become incompliant to legislation.
- Do not contain data that in case security breaches occur create great losses.

The main reasons given by FS companies to implement or do research about and use public cloud services are:

- Cost savings - From 4 times up to 200 times cheaper than traditional services.
- Flexibility - Decreased time to market
- Scalability - Improved capacity usage from 4-8% up to 70-80%

We noticed that the use of public cloud services at this moment was very small, the reasons for FS companies for this were:

- Loss of control and data ownership
- Loss of abilities to change services
- Enterprise perception (e.g. outside the perimeter you can trust none)
- Not enough guarantees on security
- Legislation issues (e.g. data location and right to audit)
- Hard to couple internal and external processes
- Low software quality in contrast to software delivered to the organization.

When summarizing the information we notice that public cloud computing is not used in core processes at banks. We see a difference with insurance companies that use public cloud computing services for a part of their sales processes. When looking at the service models used we see that the most used service models are SaaS and PaaS. The services running on these layers are mostly non-core, e-learning and testing services. At an IC we discovered that a SaaS core service was used. This service was a CRM service that contained personal data of possible clients.

At the four interviewed companies there were no IaaS services used at this moment. We found this a bit awkward as the IaaS layer gives the customer the most control about their service. When using SaaS services, most of the control is given to the cloud provider. The reason given by the IC that used the SaaS service told us this was because the SaaS solution perfectly fitted in their organization.

We also noticed differences between the two types of companies based on research in the public cloud. Banks seem to be much more careful and have a tendency to move to other type of clouds such as private and community. In contrast to this, insurance companies seem to be more open for the new developments of the public cloud and are researching serious business cases.

We explain this difference by the level of trust customers have in banks and insurance companies. The perception of customers that their money is safe at a bank is a very important reputation factor for a bank. If an incident changes this perception, it will result in reputation and trust damage which can ultimately cause a bank to go bankrupt. Bank B states that cost savings are not core business for a bank. Trust, security, and client perceptions are the main goals which may cost money. On confidentiality and integrity IC agree with this statement. Nevertheless, when we look at availability, ICs state that they have lower impacts than banks. When a service is unavailable for a couple of hours, banks will have major reputation or financial damage and may go bankrupt. At insurance companies, most of these issues can be kept internal. The few systems that are pointed to the outside world don't have high availability requirements. For this reason we think some IC's have already implemented public cloud services.

Because public cloud computing is perceived as a new technique, banks wait for reference cases of other companies making the move to the cloud. In the adoption process of public cloud computing, banks can be seen as strategic followers instead of early adopters.

When we look at the answers about the security we notice that FS companies are restrained in moving to the public cloud. We see that companies are still researching business cases for possible services. In this research risk management has a very high priority. FS companies state that the reasons for not having core services into the public cloud are mostly lack of security guarantees, trust and loss of control reasons.

We also noticed that legislation risks based on security threats were addressed by every FS company. Given this we can state that legislation is not yet evolved far enough to support the public cloud computing technique. Or the other way around, public cloud providers do not have the right measures (or do not give enough guarantees) to support FS companies.

During the interviews some information could not be obtained. For the research we tried to obtain specific information about FS security requirements. When asking the companies to go into more detail about the security requirements demanded, specific answers could not be given. The experts referred to large lists containing 500+ requirements and standards such as ISO27001, SAS 70 Type II, CobiT 4, and ISF Standards of good practice.

6 Relations Between Threats and Requirements in the FS Market

In this chapter of the thesis we describe the relations between the findings in literature and compare these with the findings in practice. We do this to answer our fourth and final sub question: What are the relations between public cloud computing, current data security threats and data security requirements in the Dutch financial service market? In order to answer this question we relate the security threats with the requirements found. By doing this, we develop insights which we underpin with the current state of cloud computing in the Dutch FS market.

6.1 Synthesis of Literature

In the first chapters of this thesis we discovered that cloud computing is a technique which is already known for years. Due to the maturity of concepts such as Internet, Web 2.0, Service oriented architecture, virtualization, etc. this technique becomes a very useful way to provide IT services and decrease costs. Cloud computing provides customers with an IT solution that makes it possible to only pay for the resources that are used. The key characteristics found in literature show that it provides on-demand self-service, resource pooling, broad network access, rapid elastic and a measured service. As can be read in chapter two, cloud computing can be implemented in several ways. For the scope of this thesis we only highlighted the public cloud as a business solution. The reason for this choice was that Capgemini specifically needed information about security in the public cloud. Capgemini is interested in the public cloud because it provides the user with all the benefits the (cloud computing) business model is able to give. Some of these benefits are the decrease of cost on capital expenses (e.g. infrastructure, hardware), the decrease of management costs, elastic capacity, the decrease of time to market, etc. A side effect of all the benefits is that this deployment model provides the customer with the most complex model in cloud computing which influences security.

In chapter three of this thesis we answer the first sub question. In literature we find that the use of a public cloud services brings some extra security threats compared to traditional IT services. Because the scope of this research is limited to data security, we only described the threats applicable to public cloud computing. We discovered that data security is applicable to every service model possible in the cloud stack. With this knowledge we chose not to make differences between the different service models (e.g. SaaS, PaaS, and IaaS). To bring order in the list of threats found in literature we chose to use the CIA model to list the threats. We compared the list of threats with the measures taken by public cloud providers and discovered that the well-known public cloud providers covered most of the threats with measures. The measures taken were validated by ISO 27001, CobiT 4.1, Safe Harbor and SAS 70 Type II audits.

In chapter four we referenced literature and information provided by the

DNB to derive the requirements for data security in the FS market. During the requirements search we discovered that a part of the requirements at FS companies were based on legislation. As our research scope is limited to Dutch FS companies, we had to take Dutch legislation into account. When analyzing the DNB framework we found that the requirements demanded by the DNB were based on the ISO 27000 and CobiT 4.1 standards.

When we look at the relations between the requirements and the threats, we see that in both cases ISO 27000 series and CobiT 4.1 standards are used. As the well-known public cloud providers are compliant to these standards, we assume that the measures taken are sufficient to mitigate the threats treated by these standards.

Using this assumption, most of the threats listed in chapter three are mitigated and security of public clouds does comply on these threats. Nevertheless, there are still two threats that are not mitigated by complying with these standards: the data location and the limited monitoring possibilities threat.

Data Location The DNB framework based on ISO27002 and CobiT 4.1 does not explicitly assess anything about data location. As the threat of the data location is based on legislation demands, we refer back to the requirements of the Dutch law. The Personal Data Protection Act directs that data may only be disclosed to third parties if they are compliant to the national provisions. This means that personal data shall be stored on locations where security requirements are at the same or higher level than obliged by Dutch laws. When this is not the case, data may not be disclosed. This indirectly means that data may not be stored at cloud providers located in a country that is not compliant to the Dutch or EU national provisions. Due to this law storing personal data in public clouds located in the US or elsewhere outside the EU is not possible. As can be read in chapter three, some public cloud providers provide the ability for customers to choose the data center location at multiple geographic regions. In this way this legislation issue can be mitigated. Another way to mitigate this threat is by using Safe Harbor principles at cloud providers. The Safe Harbor principles framework consists of a list of principles that, when followed, guarantee "adequate" security compliancy as demanded by EU privacy laws such as the Personal Data Security Act. However, there is some uncertainty on this framework; The US Patriot Act directs that any data stored on US territory must be disclosed to the government when asked for [9, 31]. Due to this law the US might not be compliant to adequate security measures. Because there is not a reference case yet, this legislation issue remains uncertain [9].

Limited Monitoring Possibilities The second threat which is not mitigated by complying with the standards is the limited monitoring possibilities threat. This threat causes many security risks for public cloud computing customers. Services become highly vulnerable for malware attacks when monitoring is not correctly applied. When looking at the DNB framework, monitoring is addressed multiple times. First of all the processes section directs that processes

should be created for monitoring breaches of regulations, law and security requirements. The technology domain of the assessment directs requirements for monitoring more in detail. Preventive, detective and corrective measures such as virus control should be in place and up-to-date. As can be read in chapter three, public cloud providers do provide services to monitor customer services. These monitoring services give insights into several parts of the services, but there remains an issue. The monitoring services are maintained by the public cloud provider and cloud customers do not have rights to audit the services themselves. When we look at legislation about this threat, we see that national authorities must be able to audit Dutch FSs. In both, Privacy and Electronic Communication Act and the Financial Supervision Act, the right to audit by national authorities is demanded.

6.2 Conclusions on Literature Findings

When we look at the relations between the threats and the requirements we see that every threat in cloud computing is applicable to requirements of services in the FS sector. A conclusion we can draw on this is that implementing services into public cloud computing will bring security risks for FS companies on all of the treats found. There are four ways of dealing with risks; avoid, control, accept, and transfer. To control these threats and lower the vulnerabilities, extra security measures have to be taken. For services that require a maximum security level, control (mitigation) on all threats has to be applied to provide the same security level as current traditional systems do. FS companies that want to use public cloud computing have to do a risk analysis on the cloud provider with the requirements found in chapter four of this thesis. By doing this, decisions can be made about the security of the data at the public cloud provider. Based on the findings of our research we state that most of the threats in public cloud computing are mitigated by cloud providers at a sufficient level. With "sufficient" we refer to the standard certificates that are awarded. Based on legislation two threats remain: Data Location and Limited Monitoring Possibilities. The Data location threat can be mitigated by selecting the correct geographical location. Leaving the Limited Monitoring Possibilities threat as one which can only be partly mitigated.

Not being able to audit the services themselves makes risk analysis on public cloud providers a hard task. In order to provide the needed audit information public cloud providers provide audit reports (SAS 70 Type II, ISO 27001, etc.) to guarantee their security. In this way the threat is partly mitigated on security requirements. However, based on legislation requirements regulators must have the right to audit FSs. This is not possible at public cloud providers and thus, the issue remains.

6.3 Relating Literature to the Practical Findings

When relating the conclusions based on literature with the practical findings we notice similarities.

For small and medium industry companies that use commodity workplaces and services, public cloud computing is a technique with large benefits. Economies of scale can be applied and costs for licenses, maintenance, and capital expenses can be lowered. This should be also the case of FS companies. In practice, we see that FS companies put effort in research about business cases with the technique. However only a small number of these business cases seem to be executed at FS companies.

By interviewing security experts, we found that the use of public cloud computing only covers a small, almost no, part of the services used at FS companies. The used public services are used because they are cheaper and more agile than on premise solutions. This underpins our findings in literature about the benefits of cloud computing. Another interesting property is that these services do not contain data that might become incompliant to legislation or might create great losses when security breaches occur.

As can be seen at the low number of public cloud services, the FS sector is very careful when moving to third parties. As already noticed in literature, it appears that giving away IT control is very hard for companies [9]. This is also the case for FS companies. Even for services in which the cloud infrastructure is more secure than their own. It is like the motorcyclist (riding the vehicle on which most accidents occur) that is scared for traveling by plane (the vehicle on which the least accidents occur) because he cannot control it. Comparing this to the findings in literature we see similarities that trust is an important factor.

To gain trust in third parties, FS companies do extensive security audits and reference certifications to be sure that cloud providers comply with their policies. Most of the time we see that if public clouds are used, well-known and experienced cloud providers (such as Salesforce.com and Amazon) are chosen. The choice for these providers is also based on trust.

Finally legislation is addressed as an important item by FS companies. Legislation such as the Personal Data Protection Act prohibits personal data to be stored at locations with "non-adequate" security measures. As directed in this act, accountability for security in public clouds remains with the organization, FS companies stay responsible for their data, even when they move it to the cloud [25, 46]. The Financial Supervision Act prohibits FS companies to use public cloud services for specific types of sensitive data. Most of the core services at FS companies contain this data. Both of these issues are underpinned by practice and are given high priorities in risk management.

During the risk analysis which is part of the risk management applied by FS companies, data security classifications are used to make distinctions between sensitive data. The data that is currently used in the public cloud services is referred to as low-risk data. This is underpinned by our findings in literature which describes that services containing data which requires maximum security levels, public cloud computing is not the right solution [23]. FS companies state

that the cost benefits of moving to public cloud computing are not enough to take the risks associated with the technique. When looking at data that has lower risks, we see that FS companies are researching and implementing public cloud services.

The fact that services with low risks are implemented is underpinned by another risk with mayor impact addressed multiple times, namely: reputation and trust damage. The fact that banks can go bankrupt in a couple of hours when trust is lost makes them very careful in using new techniques. Bank B stated that cost saving, (one of the benefits in public cloud computing) is not core business for a bank. Trust, security, and client perceptions are the main goals which may cost money. On confidentiality and integrity insurance companies agree to this statement. Nevertheless on availability issues ICs state that a large number of their products have a lower impact on reputation. Because of this, we assume that insurance companies have lower security demands which give them more opportunities to implement public cloud solutions. An example of this is the CRM service an IC is using from a public SaaS platform.

We also notice some interesting differences between the literature and practice. In literature we found that public cloud providers comply with most of the requirements of FS companies. In practice we found that FS companies use the same requirements as found in literature for auditing their third parties. When asking the companies why they do not use public cloud services their answers are: there are not enough guarantees about security. When we look at these answers, we notice that these are contra dictionary. When analyzing the other statements given during the interview we think that we should interpret "not enough guarantees" as "not a 100% trust", even when certificates are awarded. In this way we do understand their statement.

7 Conclusions and Further Research

7.1 Conclusions

In the introduction of this research we created a research question to set a goal for this research. By now we are at the point that we gathered enough information to answer this question. The main question of this research is:

> Does data security in public cloud computing comply with the data security requirements for IT services at Dutch financial services companies?

During this research we found that public cloud computing is an interesting technique which enables costs savings and agility for FS companies. But there is a catch: the new technique does not only have positives. Security is a major issue when implementing public cloud solutions. With the information gathered during the research we state that:

> Moving to cloud computing is a trade-off process between costs savings, agility and security risks. The cheaper and more agile the solution, the higher the security risks. And of course the other way around.

With this trade-off between the cloud benefits and the risks, we conclude that in situations where high levels of security are required public cloud computing cannot compete with the security of on-premise traditional services. This because the 'cheaper' public cloud solutions do not fully comply with the security standards required by companies. As the public cloud deployment model provides the cheapest computing and storage capacity, security risks are high.

When taking these insights and looking at the FS market we see that the implementation of public cloud computing for core services in FS companies is not interesting. The benefits of moving to public cloud computing are not enough to accept the risks associated with the current technique. Even when almost every important threat is mitigated by the cloud providers, FS companies will not move their core services. Loss of control, lack of security guarantees and trust in the provider are issues that expose risks which FS companies are not willing to take.

In some cases FSs in public cloud computing cannot be implemented because of legislation. E.g. Dutch legislation prohibits companies to store or process data in countries that demand lower security requirements to personal data. Another act in Dutch legislation requires FS companies to provide access to auditors of their information systems. Services that are applicable to this law cannot be placed into the public cloud.

Public cloud computing does become interesting in situations where risks (partly) can be accepted. (E.g. non-core and supporting systems) During the research we found that the CIA framework was used by FS companies to classify the data used. With this framework, acceptance of risks per type of data is

defined. By doing a risk management research at a public cloud provider a classification threshold can be set for data that may not be placed in the public cloud. With this classification organizations become able to select services that can or can't be implemented in the public cloud.

Final Conclusion As a final conclusion on the question: Does data security in public cloud computing comply with the data security requirements for IT services at Dutch financial services companies?

Partly. Data security in public cloud computing does not comply to the security requirements needed for financial services that use data which needs maximum security or have restrictions demanded by legislation. For financial services that use data with lower security classifications public cloud computing is an interesting technique because data security is sufficient.

7.2 Recommendations

To make use of the benefits in public cloud computing, considering the security of data is a must. Creating a risk management plan and doing risk analysis before implementing a public cloud service is critical. Subjects that should be included in the analysis to ensure the security of data are:

- Security policies of the cloud provider must be in line with the policies of the cloud customer.
- Cloud providers must act according to the following standards: ISO 27001, CobiT 4.1, and Safe Harbor.
- The compliance to the standards must be audited by external companies following the SAS 70 Type II standard.
- The following legislation must be taken into account: The Personal Data Protection Act, The Privacy and Electronic Communication Act, and The Financial Supervision Act.

For Capgemini this means that when using external public cloud infrastructures to deliver services to FS companies, they should include the given subjects above in their risk management and analysis. As legislation is restricting public cloud services containing sensitive financial data, core services cannot be implemented in to the public cloud. To be able to deliver these services by means of the cloud computing technique, different deployment models such as private clouds should be taken into account. As these clouds are dedicated to a single enterprise, auditing by regulators may become possible.

When looking at the competitive subjects in offering public cloud services that comply with the security demands at FS companies, Capgemini can outrun its competitors by:

- Gaining trust of their clients by providing standard certificates and external auditors;
- Gaining trust by providing guarantees by means of showing reference cases;
- Selling non-core and supporting services;

7.3 Limitations

Every research has its limitations, and so has this research. First of all, in the practical part of this research we interviewed security experts at FS companies. Due to time constraints, we only interviewed 4 experts at different FS companies. Because of this number, our conclusions might not give a representation of the whole Dutch FS sector. A larger number of interviewees and companies would improve the objectivity of this research.

The second limitation of this research is based on the background situation of the interviewees. In the practical part of this thesis, we interviewed IT security experts. The reason for this was that these people had knowledge about traditional security and cloud computing security. They have this knowledge because it is their job. This job becomes a limitation because it might create a typical mindset IT people have about cloud computing. Cloud computing is a technique and a business model that reduces costs by transferring management towards the cloud provider. This means that the number IT jobs at FS companies can be reduced and money can be saved. Talking with IT personnel about a technique that might take their job is like talking to the turkey about Christmas dinner. In this way, IT experts can have a view that might be a bit distorted. In order to prevent this, we tried to interview experts with functions located high in the organization hierarchy. Experts on this level are less affected by the threat of losing their job. We should have also interviewed a group of people with non-IT related jobs. We didn't do this because in our opinion this group did not have enough experience with the subject to answer our questions.

Another limitation in this research is the scarce literature on reference cases. The scarce literature is explained by the novelty of the technique. As already stated in the conclusions of the interviews, Dutch FS companies are strategic followers and will wait for others to go first. At this moment there are no other publicly available Dutch reference cases than our own interviews. The impact for our research is that only our own interviews can be used to validate our findings.

7.4 Discussion

When reading literature about cloud computing, talking to experts and discussing with colleagues, we see that the cloud computing for businesses hype is getting mature. Statements we hear during conferences about the subject have the same context: "cloud computing is here to stay!" We agree to this statement, but there are some critical factors that affect the success of the technique and its business case.

Looking at the hype cycle published by Gartner [53], we see that the predictions are that cloud computing will be mainstream in 2 to 5 years. When we look at the FS market, we do not agree on this. We think that the FS market is a strategic follower and will wait for others to go first. Moving back to the hype cycle, we think that public cloud computing for non-FS markets is near the slope of enlightment and cloud computing for FS markets is just past the top of the hype cycle.

During the practical research, we observed that public cloud computing is not seen as a new technique, but as a new step in outsourcing. The new differences are that in this type of outsourcing also a part of the control is outsourced.

> Giving away control is seen as a security threat and restrains FS companies to use public cloud computing.

As can be read in our conclusions, this is one of the three major reasons for not implementing the technique. In our opinion, there is a link between losing control, trust and too less guarantees. The link we notice is that because of the loss of control and the lack of guarantees, FS companies don't trust the public cloud provider to control their data. Even in situations where the public cloud providers do comply with the policies and demands about certifications.

> Due to the fact that a security officer of a FS company doesn't have the right to audit the public cloud datacenter himself, he doesn't trust it.

To be able to provide this trust, public cloud providers should provide more insights into the internal processes and grant access for auditors to the datacenters. Public cloud providers do provide guarantees about security by conducting external audits, but we think that this is not enough to satisfy the FS security officers.

Finally we found that legislation is barricade at the implementation of public cloud computing. Public cloud providers should become more open and should provide a way for customers to audit their services. As this might not always be possible, other solutions should be researched. One example of research that could be done is to apply changes in legislation or create legislation which is applicable to the technique as is discussed in [54].

7.5 Further Research

We believe that this research provides an initial foundation for reference cases of public cloud computing in the Dutch FS market. Further research on this topic will improve and underpin the conclusions of this research. A larger group of FS companies will provide more strength to the conclusions. Several other fields of research can be interesting to explore on this research subject.

- First, cloud computing is a technique which is still undergoing an evolution phase, we see new interesting subjects such as certifications at cloud providers. These certifications provide customers with the assurance that security measures are in to place and that more security sensitive services can be placed in the cloud. The maturity of these certifications and security measures should be validated.
- In the field of securing the cloud we see different new techniques that might increase data security in the public cloud such as homomorpic encryption [55] (a technique that enables processing on encrypted data) and Self-Cleansing Intrusion Tolerance (SCIT) [56] (a technique that switches machines on and off in a way that attackers don't get enough time to do damage).
- In literature we found that there is no common industry cloud computing security standard to benchmark cloud providers' security [9]. Further research on this subject is needed to be able to make a well underpinned choice of choosing a cloud provider.
- During this research we noticed that FS companies state that public cloud computing is a step to far. Keeping their opinions in mind, it seems more likely that FS companies choose private or community clouds. As this research focused on public clouds only, we did not include other deployment models. Research may reveal that these models may have interesting business opportunities for FS companies.

References

[1] L.M. Kaufman. Data security in the world of cloud computing. *IEEE Security and Privacy*, 2009.

[2] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 2011.

[3] Capgemini. Capgemini about us. http://www.nl.capgemini.com/over-ons/, 2010.

[4] Capgemini. Way of working 2010 - financial services, 2010.

[5] L. M. Vaquero, L. R. Merino, and M. Caceres, J.and Lindner. A break in the clouds: towards a cloud definition. *SIGCOMM Comput. Commun. Rev.*, 39, 2009.

[6] M.D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis, and A. Vakali. Cloud computing: Distributed internet computing for it and scientific research. *Internet Computing, IEEE*, 2009.

[7] J. Staten. Is cloud computing ready for the enterprise? *Forrester Research*, 2008.

[8] L. M. Kaufman. Can public cloud security meet its unique challenges? *IEEE Security and Privacy*, 8, 2010.

[9] Center for the protection of national infrastructure (CPNI). Cloud computing. *Information Security Briefing*, 2010.

[10] U. Faisst and O. Prokein. An optimization model for the management of security risks in banking companies. *E-Commerce Technology, IEEE International Conference on*, 2005.

[11] N. Kroes. Cloud computing and data protection. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/686&format=PDF&aged=0&language=EN&guiLanguage=en, 2010. Accessed at 26 November 2010.

[12] International Data Corporation. New idc it cloud services survey: Top benefits and challenges. http://blogs.idc.com/ie/?p=730, 2009. Accessed at 24 March 2011.

[13] KPMG. From hype to future. http://www.kpmg.com/NL/nl/IssuesAndInsights/ArticlesPublications/Doc
IT%20Performance/From_Hype_to_Future.pdf, 2010. Accessed at 20 April 2011.

[14] National Security Telecommunications and Information Systems Security Committee. Infosec glossary. http://security.isu.edu/pdf/4009.pdf, 200. Accessed at 15 December 2010.

[15] P. Verschuren and H. Doorewaard. *Designing a Research Project*. LEMNA, 2005.

[16] M. Menzel, R. Warschofsky, I. Thomas, C. Willems, and C. Meinel. The service security lab: A model-driven platform to compose and explore service security in the cloud. *Services, IEEE Congress on Services*, 2010.

[17] G. Zhao, Z. Rong, M.G. Jaatun, and F.E. Sandnes. Deployment models: Towards eliminating security concerns from cloud computing. *High Performance Computing and Simulation (HPCS)*, 2010.

[18] D. Molnar and S. Schechter. Self hosting vs. cloud hosting: Accounting for the security impact of hosting in the cloud, 2010.

[19] S. Ramgovind, M.M. Eloff, and E. Smith. The management of security in cloud computing. *Information Security for South Africa (ISSA)*, 2010.

[20] C. Tsai, U. Lin, A.Y. Chang, and C. Chen. Information security issue of enterprises adopting the application of cloud computing. *Networked Computing and Advanced Information Management (NCM)*, 2010.

[21] J. Brodkin. Gartner: Seven cloud-computing security risks. http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,0, 2008. Accessed at 15 December 2010.

[22] ENISA. Security & resilience in governmental clouds. *ENISA*, 2011.

[23] D. S. Linthicum. *Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide*. Addison-Wesley Professional, 1st edition, 2009.

[24] P. Mell and T. Grance. Working definition of cloud computing v15. http://csrc.nist.gov/groups/SNS/cloud-computing/index.html, 2009. Accessed at 1 December 2010.

[25] W. Jansen and T. Grance. Draft: Guidelines on security and privacy in public cloud computing. *NIST Draft Special Publication 800-144*, 2011.

[26] Capgemini. Whitepaper: Simplify your journey to the cloud. *About the cloud*, 2010.

[27] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. Above the clouds: A berkeley view of cloud computing. Technical report, EECS Department, University of California, Berkeley, 2009. Accessed at 23 April 2011.

[28] The Economist. Tanks in the cloud. http://www.economist.com/node/17797794, 2010. Accessed at 24 May 2011.

[29] Amazon. Aws economics. http://aws.amazon.com/economics/, 2011. Accessed at 11 March 2011.

[30] C. Wang. How secure is your cloud. *Forrester for Security & Risk Management Professionals*, 2009.

[31] A. Sangroya, S. Kumar, J. Dhok, and V. Varma. Towards analyzing data security risks in cloud computing environments. *International Conference on Information Systems, Technology, and Management (ICISTM 2010)*, 2010.

[32] C. P. Pfleeger and S. L. Pfleeger. *Security in Computing (4th Edition)*. Prentice Hall PTR, 2006.

[33] D. Catteddu. Cloud computing: Benefits, risks and recommendations for information security. Springer Berlin Heidelberg, 2010.

[34] K. Popovic and Z. Hocenski. Cloud computing security issues and challenges. *MIPRO: Proceedings of the 33rd International Convention*, 2010.

[35] Tweakers.net. Google gmail problemen zijn definitief voorbij. http://tweakers.net/nieuws/73022/google-gmail-problemen-zijn-definitief-voorbij.html, 2011. Accessed at 24 March 2011.

[36] Amazon. Amazon webservices security. http://aws.amazon.com/security/, 2011. Accessed at 25 April 2011.

[37] C. Kaufman and R. Venkatapathy. Windows azure security overview. http://www.globalfoundationservices.com/security/documents/WindowsAzureSecurityOverview1_0Aug2010.pdf, 2010. Accessed at 28 March 2011.

[38] Microsoft Global Foundations. Securing microsoft's cloud infrastructure. http://www.globalfoundationservices.com/security/documents/ SecuringtheMSCloudMay09.pdf, 2009. Accessed at 28 March 2011.

[39] Salesforce.com. Trust - salesforce.com. http://trust.salesforce.com/trust/security/, 2011. Accessed at 20 April 2011.

[40] M. Vrancianu and L.A. Popa. Considerations regarding the security and protection of e-banking services consumers interests. *The AMFITEATRU ECONOMIC journal*, 2010.

[41] D. Fink. A security framework for information systems outsourcing. *Information Management & Computer Security Vol.2 No.4 pp. 3-8*, 1994.

[42] G. F. Knolmayer and P. Asprion. Assuring compliance in it outsourcing relationships: Frameworks and selected applications. *Institute of Information Systems, University of Bern*, 2011.

[43] Cloud Security Alliance CSA. Security guidance for critical areas of focus in cloud computing v2.1. 2009.

[44] De Nederlandsche Bank. Assessment framework for dnb information security investigation. http://www.dnb.nl/openboek/extern/id/en/all/41-198417.html, 2010. Accessed at 13 January 2011.

[45] J. Ruiter and M. Warnier. Privacy regulations for cloud computing. *TU Delft*, 2010.

[46] European Commission. Directive 95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf, 1995.

[47] European Union. Safe harbour privacy principles. http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do?uri=CELEX%3A32000D0520%3AEN%3AHTML, 2000. Accessed at 28 March 2011.

[48] European Commission. Directive 2009/136/ec of the european parliament and of the council of 25november 2009. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF, 2009.

[49] De Nederlandsche Overheid. Wet op het financieel toezicht. http://wetten.overheid.nl/BWBR0020368/1/geldigheidsdatum_04-05-2011, 2006. Accessed at 2 December 2010.

[50] De Nederlandsche Bank. Register financiele ondernemers. http://registers.dnb.nl/nl/professionals/registers/alle-huidige-registers.aspx?dnb=1, 2011. Accessed at 11 January 2011.

[51] NRC Handelsblad. Klassieke bankrun werd dsb fataal. http://vorige.nrc.nl/economie/article2384696.ece/Bankrun_werd_DSB_fataal, 2009. Accessed at 28 March 2011.

[52] SAP. Sap solution composer. http://solutioncomposer.sap.com, 2011. Accessed at 11 January 2011.

[53] Gartner. Gartner's 2010 hype cycle special report evaluates maturity of 1,800 technologies. http://www.gartner.com/it/page.jsp?id=1447613, 2010. Accessed at 21 Februari 2010.

[54] P. Van Der Beek. Kroes pleit voor eu-regels cloud computing. http://www.computable.nl/artikel/ict_topics/cloud_computing/3856334/2333364/kroes-pleit-voor-euregels-cloud-computing.html, 2011. Accessed at 2 December 2010.

[55] C. Fontaine and F. Galand. A survey of homomorphic encryption for non-specialists. *EURASIP J. Inf. Secur.*, 2007.

[56] D. Arsenault, A. Sood, and Y. Huang. Secure, resilient computing clusters: Self-cleansing intrusion tolerance with hardware enforced security (scit/hes). *The Second International Conference on Availability, Reliability and Security (ARES'07)*, 2007.

[57] Amazon. Amazon ec2. http://aws.amazon.com/ec2/, 2011. Accessed at 21 March 2011.

[58] Tripwire. Leveraging the iso 27000 standards to fast track and complement pci dss. http://www.tripwire.com/en/emea/register/981561?cat=PCI&type=wp, 2011. Accessed at 25 April 2011.

[59] SAS 70. Sas 70 overview. http://sas70.com/sas70_overview.html, 2011. Accessed at 25 April 2011.

[60] C.G. Nickell and C. Denyer. An introduction to sas 70 audits. *BENEFITS LAW JOURNAL Vol 20*, 2007.

[61] ISACA. Cobit 4.1 exerpt. http://www.isaca.org/KnowledgeCenter/cobit/Documents/COBIT4.pdf, 2007. Accessed at 2 May 2011.

[62] NIST. Guide for mapping types of information and information systems to security categories. *Volume I, SP 800-60 Rev. 1.*, 2008.

Part I
Appendices

Contents of Part I

A Explorative Survey

To get some orientation for my research, we held a survey during a congress called: Landelijk Architectuur Congres (LAC). On this congress mostly architects were present, we questioned 46 of them. We chose to do this survey to get more insights in what the hot topics at this moment are. The following sections show a summary of the survey with the most interesting questions.

Questions

To get an idea to which extend cloud computing is already used and applied in businesses we asked what public and private cloud computing applications, platforms and infrastructures where used by the respondent companies.

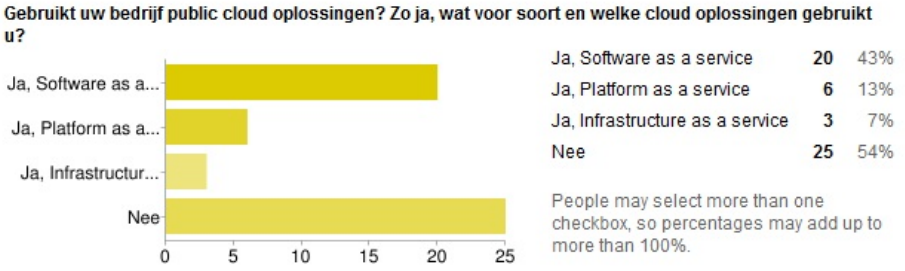

Figure 14: Use of public cloud services

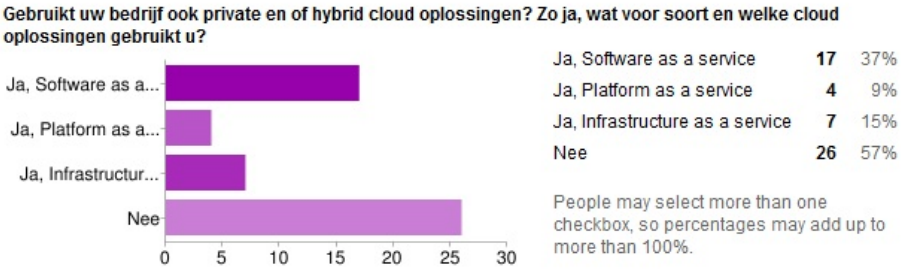

Figure 15: Use of private or hybrid cloud services

As seen in figure 14 almost half of the interviewed companies do not use public cloud services. In figure 15 you can see that this is almost the same for private and hybrid cloud computing. When we combine these two questions we see that 16 of the 46 respondents don't use cloud computing at al. Other interesting conclusions we can generate out of these answers is that SaaS solutions are the mostly used services under the respondents.

The respondents that used cloud services gave cost savings as main reason for using cloud services. Scalability & flexibility was the second most popular reason to make use of cloud services. Time to market and availability got the shared third place as can be seen in figure: 16.

Figure 16: Reasons for choosing cloud services

The respondents that did not use cloud computing services gave in most of the time their own reasons for not using cloud services, see figure 17. In these answers we found a trend which was that the cloud computing hype was too new at this moment and the respondent companies would rather wait than be one of the first adaptors.

Figure 17: Why not use cloud services

On the question: On which of the following security issues are you most concerned when using cloud services? integrity and confidentiality score very high, see figure: 18. With this question we find that confidentiality and integrity are very important security issues in cloud computing and these have to be taken into account in my research.

When we asked the next question we got some answers which I didn't expect. This question was: Is the security in your datacenter better organized than the security at cloud provider services? After the previous question, we would have expected that most of the respondents would have answered yes, but it came out that almost 2/3 answered no, see figure: 19. When we checked the answers they gave we found that there were only a few explanations for choosing no, the explanation that came up front was that small companies didn't have the expertise to secure their datacenters in a way cloud providers could. The

Figure 18: On which security issues are you most concerned

respondents choosing yes explained that they had own control over their data (digital as physical) and had control over their firewalls.

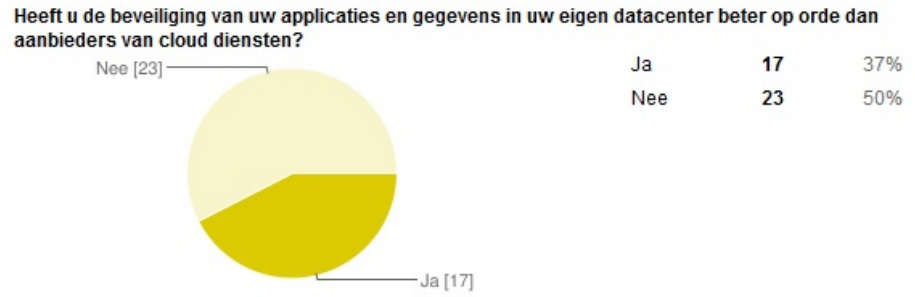

Figure 19: Is your own datacenter security better organized than the security at cloud provider services?

Filtering Results

Because the research scope will be limited to the financial service market, we also asked the respondents in which sector they were working to be able to differentiate between them. The answers of this question are summarized in figure: 20.

The answers were a little bit disappointing, we only got 4 specific financial service market respondents (2 banking, 2 insurance). When looking at this specific group, we noticed some changes in the diagrams generated out of the answers. First of all, we found that public cloud computing services are less used in these sectors the same can be concluded for private cloud computing which wasn't used at al.

The answers on the questions about why choose or not choosing for cloud computing were even more disappointing. Some people did not answer these questions and the result we got was that the time to market was the main reason for using cloud computing. The reasons for not choosing cloud computing services had the same problem, results on this question were: change costs and not willing to be the first to move to cloud. Finally in this group opinions about the security of their own datacenter in contrast with the cloud service provider

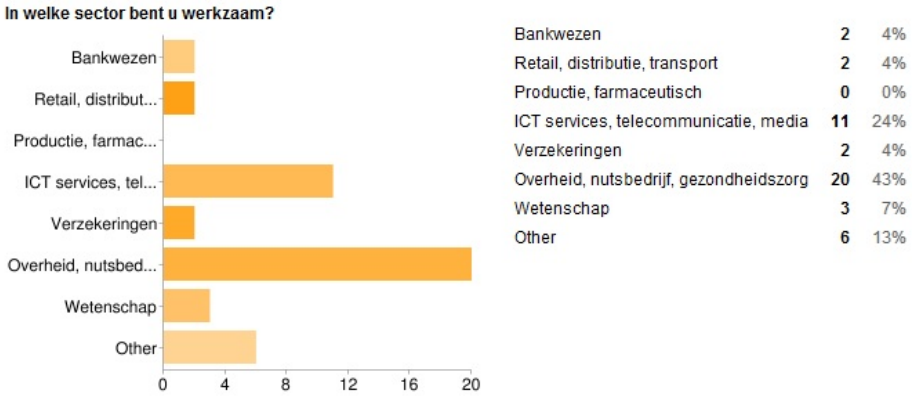

Figure 20: In which sector are you working?

show a 50/50%. When looking at the extending answers why this is the case: self-control, ownership and emotionally were the answers.

Conclusion

As conclusions of this small orientation survey we can say that the interviewed group of 46 architects, from which 4 of the target group. Because the target group is too small to get some orientation, we used the full group of respondents. We found that this group:

- uses both private (or hybrid) and public cloud computing. (Except the public and finance sector)
- SaaS solutions are mostly used.
- believes that cost aspects, flexibility and scalability are the main reasons for choosing cloud solutions.
- does not use cloud computing because it is too new, don't wants to lose control and security is lacking.
- believes that integrity and confidentiality are the main security issues in cloud services.
- believes that their datacenter is more secure than the datacenter of cloud providers.

For this research this means we have to take a look at security in public cloud computing because it looks like the target group is starting to use this. We notice that the number of cloud services in the FS group is not large because the technique is too new and respondents want to stay in control. Integrity and confidentiality will be the main security aspects to look for, because these are believed the most important security aspects of cloud services.

B Pay-per-use Model

To give an overview about the way cloud providers deploy their services, we give an example of a well-known cloud provider. At the moment the number of cloud computing providers is rising, this means there are also different services models that are sold. In this example we chose Amazon's EC2 cloud model to give an example of the pay-per-use model.

The pay-per-use model is a model that characterizes public cloud computing services. Even in the cloud computing definition pay-per-use is mentioned. As a customer of a cloud provider this model means that you only pay for the amount of computing power, data bandwidth, or MB's RAM you used. In [57], Amazon publishes its pricing information on this model.

The pricing model is divided into multiple instance types that separate themselves by the way that they are used. Amazon uses different instances based on micro, standard, high memory, high CPU usage, high GPU, and cluster instances [57]. An example of a default standard instance is a virtual machine with:

- 1.7 GB memory
- 1 EC2 Compute Unit (1 virtual core with 1 EC2 Compute Unit)
- 160 GB instance storage
- 32-bit platform
- I/O Performance: Moderate

Amazon uses Compute units to define their virtual CPU's. Their definition of 1 EC2 Compute unit is:

> One EC2 Compute Unit provides the equivalent CPU capacity of a 1.0-1.2 GHz 2007 Opteron or 2007 Xeon processor. This is also the equivalent to an early-2006 1.7 GHz Xeon processor [57].

Each instance has different billing prices. There are also differences in on-demand, reserved, and on spot instances [57]. To give an indication of the prices for the default standard on-demand instance are: $0.095 per hour for a Linux instance and $0.12 per hour for a Windows instance.

Because these costs are only cost for usage of the virtual machine, data transfer costs have to be added. The prices for data transfer at Amazon are: Up to 10 TB per Month $0.150 per GB in US & EU regions[57].

C ISO 27000

In this chapter we go into more detail about the ISO 27000 standards. This text is directly copied from [58].

The standards

The ISO 27000 standards are a series of interrelated standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). These standards provide best practice recommendations for protecting an organization and its information assets from the inherent business risks that can result from an asset's loss of availability, confidentiality and integrity. The standards are based on the principles of risk assessment and the implementation of controls and security measures to appropriately protect information assets against the identified risks.

ISO 27001 describes the requirements of an Information Security Management System (ISMS) that is based on the Plan, Do, Check, Act ("PDCA") methodology. The purpose of this methodology is to continuously improve the quality of the management system of all ISO standards, and not just the ISO 27000 series. An ISMS is a set of policies with the intent of effectively managing information security by designing, implementing, maintaining, and constantly improving a structured, security-driven set of processes and systems. These policies should greatly reduce an organization's information security risks and ensure a business aligns with the industry-wide "CIA" concept of maintaining the confidentiality, integrity and availability of information assets at all times. The organization must define and document the areas that are included in the ISMS in a "Scope of Applicability."

In practice, defining the scope requires organizations to possess deep knowledge of the environment to be protected-the "in-scope" environment. ISO 27002 is a code of practice for information security management designed to assist organizations with implementing an ISMS. The current standard is a close revision of the British Standard (BS) 7799-1 that was published in 1999 and organized across 11 domains. Each domain covers key security points the entity needs to address.

Domains

Security Policy The main security document that covers overall security guidelines such as Authentication, Authorization, Data Protection, Internet Access, Internet Services, Security Audit, Incident Handling and Responsibilities. The Security Policy is a high-level document that should be easy to understand and implement. The document is typically ratified and sponsored by top-level management.

Organization of Information Security Aims to ensure that the entity creates a detailed security infrastructure with internal security zones and external

zones that restrict third party access to facilities or office premises. Also addresses creating contracts/agreements created for outsourced data processing to ensure contracted organizations apply guidelines outlined in the detailed security infrastructure.

Asset Management Ensures assets are assigned a security value and classification that dictates how they should be protected. Assets are typically defined as people, information assets (such as paper and electronic documents), software and Intellectual property (intangible assets), physical assets, services or processes, and corporate branding and reputation.

Human Resources Security Aims to ensure that background of those who work for the organization is checked and that all staff, whether permanent, part-time or outsourced do not pose a security threat to the organization's assets. Human resources security is implemented by controlling the recruitment process, providing ongoing staff training with respect to security, and implementing an incident response plan where all staff members have a role.

Physical and Environmental Security A secure working environment includes protection of all physical assets from security hazards. These protective measures force entities to implement access control to physical and intangible assets.

Communications and Operations Management Relates to documentation surrounding security procedures for all organizational operations. Communications and operations management requires entities to establish procedures for incident logging, back-up of information assets, enforcement of network security controls, and creation of procedures for inter-organizational data exchange.

Access Control Covers management of access to information assets and to computer networks, as well as operating system- and application-level systems. It also includes provisions on logging and monitoring system usage, and specific requirements on protecting mobile and teleworking assets.

Information Systems, Acquisition, Development and Maintenance Provides guidelines for acquiring systems used to process, store or transmit information, as well as security provisions to prevent systems from becoming a threat to the confidentiality, integrity or availability of assets. This domain also includes a development and maintenance emphasis, which requires entities to identify system security requirements and mitigate system threats at any stage of the system lifecycle by using security techniques such as cryptography that protect information during any stage of the system life cycle. Ensures organizations create methods or procedures to protect system and other important files and to control the development and maintenance of systems by implementing security during lifecycle (SDLC) of systems.

Information Security Incident Management Deals with the structure required for the entity to prevent security incidents from happening and to deal with them should incidents take place. A plan is developed and implemented that covers any possible threats against assets and identifies how the entity will mitigate an incident or investigate an incident if one occurs.

Business Continuity Management Describes the process the entity will use to ensure that mission critical assets are always available to authorized staff.

Compliance Ensures the entity is in compliance with any applicable legal or industry security framework or standard that applies to its in-scope environment.

D SAS 70

In this chapter, the SAS 70 Auditing Standard is explained into more detail. Most of this text is directly copied from the SAS 70 website [59] and from [60].

The Auditing Standard

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A service auditor's examination performed in accordance with SAS No. 70 (also commonly referred to as a "SAS 70 Audit") is widely recognized, because it represents that a service organization has been through an in-depth audit of their control objectives and control activities, which often include controls over information technology and related processes. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers.

SAS No. 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. The issuance of a service auditor's report prepared in accordance with SAS No. 70 signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. The service auditor's report, which includes the service auditor's opinion, is issued to the service organization at the conclusion of a SAS 70 examination.

SAS No. 70 provides guidance to enable an independent auditor ("service auditor") to issue an opinion on a service organization's description of controls through a Service Auditor's Report. SAS 70 does not specify a pre-determined set of control objectives or control activities that service organizations must achieve. Service auditors are required to follow the AICPA's standards for fieldwork, quality control, and reporting. A SAS 70 Audit is not a "checklist" audit.

SAS No. 70 is generally applicable when an independent auditor ("user auditor") is planning the financial statement audit of an entity ("user organization") that obtains services from another organization ("service organization"). Service organizations that impact a user organization's system of internal controls could be application service providers, bank trust departments, claims processing centers, data centers, third party administrators, or other data processing service bureaus.

The Audit

The SAS 70 report is based on an in-depth audit of the internal controls of the organization and serves to demonstrate that adequate controls and safeguards for hosting or processing client data are in place. Because of the very specialized nature of SAS 70 audits, not the entire organization does go through an audit.

Instead, the identified platform or platforms that are currently being used to conduct activities related to user organizations is what will be audited, along with other areas deemed vital by the auditor. During the audit standards such as ISO 17799, COBIT, and FFIEC are used. Example business controls that are tested during an audit are:

- Organizational
- Application development and maintenance
- Logical security and access
- Physical security and access
- Application controls
- System maintenance controls
- Data processing controls
- Business continuity controls

The Audit Types

There are two types of audits, called Type I and II. The main difference between the two types is that Type II requires a testing period. Usually this time frame is no less than six months. In this timeframe tests are conducted on an organizations control environment. A Type I audit only applies for a specified date, not testing period is addressed.

E COBIT

In this chapter, the COBIT Standard is explained into more detail. Most of this text is directly copied from the COBIT excerpt document [61].

The Framework

The COBIT framework provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's good practices represent the consensus of experts. They are strongly focused more on control, less on execution. These practices will help optimize IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong. For IT to be successful in delivering against business requirements, management should put an internal control system or framework in place. The COBIT control framework contributes to these needs by:

- Making a link to the business requirements
- Organizing IT activities into a generally accepted process model
- Identifying the major IT resources to be leveraged
- Defining the management control objectives to be considered

The business orientation of COBIT consists of linking business goals to IT goals, providing metrics and maturity models to measure their achievement, and identifying the associated responsibilities of business and IT process owners. The process focus of COBIT is illustrated by a process model that subdivides IT into four domains and 34 processes in line with the responsibility areas of plan, build, run and monitor, providing an end-to-end view of IT. For a graphical representation of this model we refer to figure 21. Enterprise architecture concepts help identify the resources essential for process success, i.e., applications, information, infrastructure and people. In summary, to provide the information that the enterprise needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.

Domains

PLAN AND ORGANISE (PO) This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. The realization of the strategic vision needs to be planned, communicated and managed for different perspectives. A proper organization as well as technological infrastructure should be put in place. This domain typically addresses the following management questions:

- Are IT and the business strategy aligned?
- Is the enterprise achieving optimum use of its resources?

- Does everyone in the organization understand the IT objectives?
- Are IT risks understood and being managed?
- Is the quality of IT systems appropriate for business needs?

ACQUIRE AND IMPLEMENT (AI) To realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives. This domain typically addresses the following management questions:

- Are new projects likely to deliver solutions that meet business needs?
- Are new projects likely to be delivered on time and within budget?
- Will the new systems work properly when implemented?
- Will changes be made without upsetting current business operations?

DELIVER AND SUPPORT (DS) This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and operational facilities. It typically addresses the following management questions:

- Are IT services being delivered in line with business priorities?
- Are IT costs optimized?
- Is the workforce able to use the IT systems productively and safely?
- Are adequate confidentiality, integrity and availability in place for information security?

MONITOR AND EVALUATE (ME) All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance and governance. It typically addresses the following management questions:

- Is IT's performance measured to detect problems before it is too late?
- Does management ensure that internal controls are effective and efficient?
- Can IT performance be linked back to business goals?
- Are adequate confidentiality, integrity and availability controls in place for information security?

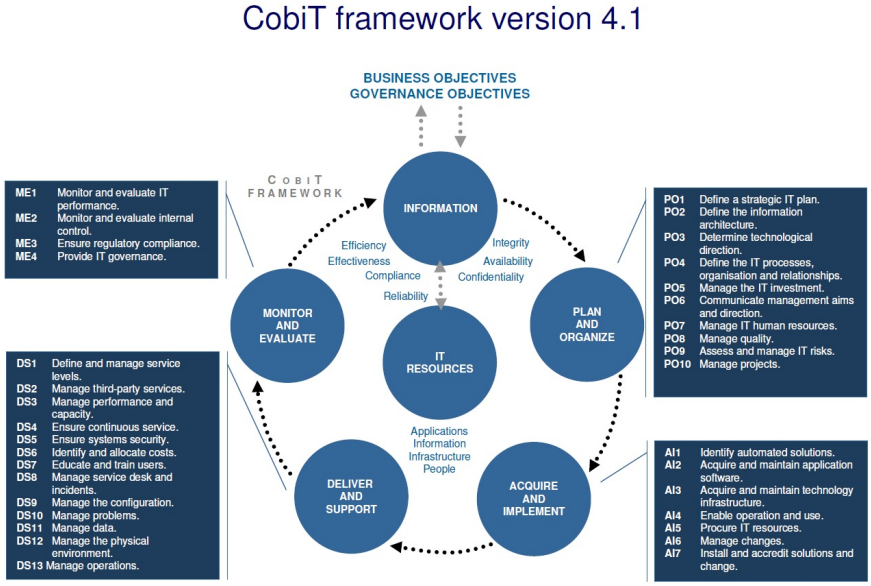

Figure 21: Overall COBIT Framework

F Safe Harbor

In this chapter, the safe harbor framework is explained into more detail. Most of this text is directly copied from legislation literature [47].

Framework

The European Union's comprehensive privacy legislation, the Directive on Data Protection (the Directive), became effective on October 25, 1998. It requires that transfers of personal data take place only to non-EU countries that provide an "adequate" level of privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. Given those differences, many U.S. organizations have expressed uncertainty about the impact of the EU-required "adequacy standard" on personal data transfers from the European Union to the United States.

To diminish this uncertainty and provide a more predictable framework for such data transfers, the Department of Commerce is issuing this document and Frequently Asked Questions ("the Principles") under its statutory authority to foster, promote, and develop international commerce. The Principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They

are intended for use solely by U.S. organizations receiving personal data from the European Union for the purpose of qualifying for the safe harbor and the presumption of "adequacy" it creates.

Decisions by organizations to qualify for the safe harbor are entirely voluntary, and organizations may qualify for the safe harbor in different ways. Organizations that decide to adhere to the Principles must comply with the Principles in order to obtain and retain the benefits of the safe harbor and publicly declare that they do so. For example, if an organization joins a self-regulatory privacy program that adheres to the Principles, it qualifies for the safe harbor. Organizations may also qualify by developing their own self-regulatory privacy policies provided that they conform with the Principles.

Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive of Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts.

Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.

Principles

NOTICE An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

CHOICE An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice. For sensitive information (i.e.

personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party identifies and treats it as sensitive.

ONWARD TRANSFER To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

SECURITY Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

DATA INTEGRITY Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

ACCESS Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

ENFORCEMENT Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

G Interview Framework

To get information about the state of the art of cloud computing in the Dutch FS market, we searched for literature about the subject. As cloud computing is a very new technique and companies in the FS market are not early adopters it is very hard to find case studies about implementations of cloud computing in this sector. To get to this information interviews have to provide us with the information we need. This section will provide the reader with a framework in which the interview questions, methodology, approach and interviewees will be described.

Objectives

The interviews will be conducted to achieve the following objectives:

- define current usage of public cloud computing services in FS companies;
- define security reasons for (not) implementing cloud computing services in FS companies;
- enable contact for validation of findings;

Methodology

The interviews will be conducted in 90 minutes time. The interviewees are not given any information about the findings in literature. The only information they get is about the background of the research and the definitions of terms used in the interview. The reasons not to give them this information are because:

- We don't want to influence their opinion or information they will give to us.
- We assume that most interviewees don't have time to read the theoretical findings on beforehand.

All interviews will be recorded and notes will be taken. The notes will be used as a base for the analysis. As things become unclear the recordings become useful to listen things back. Every interview will be analyzed separately and has to be validated by the interviewees before it will be used in the thesis. The interviews will take place between the 1 of March and the 1 of April.

Approach

In the interviews, the following subjects will be treated in the given sequence.

- Acquaintance - to get to know each other, job, function, role, experience etc.;
- Explain definitions and theoretical model for research;

- Explain goal of research;
- Ask questions
- Wrap up:
  - Summarize answers
  - Initiate future contact for validation.

Interview Questions

Experience and role of interviewee

- Whtat is your role in the organization?
- For how long are you doing this job?
- What are your personal and business experiences with cloud computing?

The Dutch FS market

- What percentage of services in your datacenter would have benefits from elastic computing capacity? (What services are these?)
- What percentage of services in your datacenter would have benefits from elastic storage capacity? (What services are these?)
- How do you calculate the cost of a service in your datacenter?
- What are the total costs for the usage of 1GB RAM/hour in your datacenter? and 1GB storage/hour?

Public Cloud Computing in Dutch FS companies

- What developments in the field of public cloud computing are active at this moment in your business?
- Which public cloud services are used in your company?
- In which processes are these services used?
  - Bank
    - Sales & Service (e.g. simulating product performance)
    - Cash and Liquidity Management (e.g. personalized services such as support, faqs, etc.)
    - Cash and Liquidity Management (e.g. payment transactions)
  - Insurance Company
    - Sales (e.g. product offering services)

        * Policy Administration (e.g. premium/benefit calculation services)
        * Claims (e.g. services that settle claims)

- For how long do you already use these services? Are these services in production, or are you still testing? Pilots?
- What are the reasons to switch to public cloud services?
- What are the main reasons for not switching?

Data security risks in Public Cloud Computing

- What is the view of your company about the risks of information security in public cloud computing?
- What measures do you take to mitigate risks when using public cloud computing?
- Do you use classifications in data security for specific processes, applications or data? If so, what are they?
- Is there a classification that indicates that a process or data cannot be used in the cloud?
- What security requirements do you demand from IT services in the field of data security? Are there differences between requirements in classifications?
- How do you check if IT services comply with this?

Cases

- Which of the following processes in your company are or could be placed into the public cloud, when looking at data security? Why? (What classifications?)
    - Bank
        * Sales & Service (e.g. simulating product performance)
        * Cash and Liquidity Management (e.g. personalized services such as support, faqs, etc.)
        * Cash and Liquidity Management (e.g. payment transactions)
    - Insurance Company
        * Sales (e.g. product offering services)
        * Policy Administration (e.g. premium/benefit calculation services)
        * Claims (e.g. services that settle claims)

H Classification of Data

As data security requirements cannot always be fulfilled (e.g. costs, legislation), decisions about the compliance of the security requirements have to be made. A critical issue in this selection process is that the types of data processed and stored at the service providers have to be classified. An example provide by ENISA describes that in public organizations four types of data classifications are used: Personal data (e.g. names, addresses), sensitive data (e.g. intellectual property, business confidential and financial transaction data), classified information, and aggregated data. All these classifications have their own security requirement and risk acceptance specifications.

To be able to make these distinctions, the types of data used and the impact when security measures fail have to be identified.

There are different ways to classify the data, in [62] a guide to map types of information and information systems to security categories is described. In this guide a distinction is made on CIA security objectives and impact levels. For every type of data an impact level based on confidentiality, integrity and availability is made. These are combined to specify a security classification. The process is depicted in figure 22.

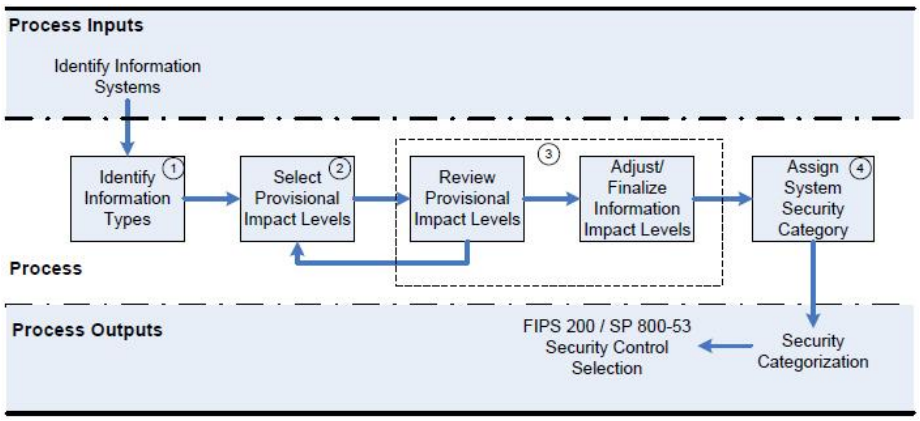

Figure 22: Security Categorization Process [62]

The product of the categorization process is a list of categories in which data can be classified. A very simple and generic model example of such a list could be:

- Level 3: High sensitive data is classified as C = 5, I = 5, A = 5.
- Level 2: Medium sensitive data is classified as C = 3, I = 3, A = 3.
- Level 1: Low sensitive data is classified as C = 1, I = 1, A = 1.