Strategy for the use of Cloud Computing

Student:
Steven de Bruijn
Radboud Nijmegen, 2011

Supervisor:
Prof. dr. ir. Th. P. van der Weide
Dep. of Computer Science
Radboud Nijmegen, 2011

Second Supervisor:
Dr. K. Kursawe
Dep. of Computer Science
Radboud Nijmegen, 2011

February 15, 2011

Master thesis code: 142IK

Contents

1 Introduction

A way for companies to distinguish themselves from other companies is through innovation, as has been showed in recent studies[**?**]. An example of innovation is technological development. Developments in the enviroment of companies come at a rapid pace. The latest trends in computer science are a result of these developments. The amount of information required to make decisions increases and thereby the time to make a decision increases as well [**?**], but for companies this is business as usual. Often companies find it hard to make the right decision whether or not to implement a new technology or not.

A new technology has emerged named Cloud Computing. Cloud Computing technology differs from other technologies, like Client/Server model. Client-server model of computing is a distributed application structure that partitions tasks or workloads between service providers, called servers, and service requesters, called clients[**?**]. Cloud Computing refers to the services that are provided to a customer over the internet, this involves hardware and software of that services in a datacenter [**?**]. Cloud Computing distinguishes itself from client server model by taking over the entire service.

Cloud Computing can offer a lot of possibilities for companies[**?**]. An company that uses Cloud Computing does not need to worry any longer about potential hardware and software issues. A company leaves those issues up to a cloud provider (The Company that offers the cloud). Cloud Computing can be separated into four layers. A layer is a different function that the cloud provider offers to companies, ranging from hardware, software, platform and the data layer. Cloud Computing can offer advantages to companies because they do not need to worry about the different issues with the layers. An example of an advantage is that the company does not need to worry about which operating system has to be chosen or what kind of hardware needs to bought.

Cloud Computing is a hot topic and there are many different opinions about the usage of this technology. [**?**]. The choice whether to switch over to a cloud provider is hard to make for companies. Moreover, companies have to take into consideration what type of cloud they are going to use. The costs for companies that want to manage their own datacenter are high. The solution that Cloud Computing provides also takes away the necessity for companies to choose between platforms, applications or hardware.

Costs reduction is always a big issue, therefore, companies might find the solution Cloud Computing provides very interesting. Further, flexibility is very important for companies because businesses must be able to react rapidly on developments in order to follow the market changes[**?**]. An example is the credit crisis. When a company can adapt to the fast changes, this will mean they can survive in difficult times. Since the credit crisis, businesses get a lot less requests and invoices from customers or other parts that are linked to business

processes. This will have an effect on the IT- environments of companies because the usage of the datancenter is lower. This results into large overhead costs.

Companies can save money and other resources when they switch to Cloud Computing because the operational tasks are taken over by the cloud provider. Examples of operational costs are maintenance of software and hardware, and the employees that have to perform these tasks[**?**].When companies use Cloud Computing they only have to pay for the services that they use. A decrease in capacity entails less costs. For example, when there is no more hard disk space or there is the need for more CPU power this needs to be bought. This will take some time because the hardware needs to be ordered and installed. When using Cloud Computing these issues are solved in a different way; it is possible to increase CPU power of storage capability within 10 minutes. With this possibility in an IT-landscape it can provide more scalability. Also, the costs will decrease dramatically and it is easy to scale down[**?**].

There are two broad categories of clouds, Public and Private Cloud. In a private cloud the cloud infrastructure is operated solely for one company. It can either be managed by the company or a third party and may exist on premise or off premise[**?**]. In a public cloud the cloud infrastructure is made available to the general public or a large industry group and is owned by cloud provider [**?**]. The difference between the two terms is that private Cloud Computing is for one company only and private cloud is for more than one company. A characteristic of public Cloud Computing is resource sharing. Facebook for example of public Cloud Computing, has the data of multiple users on one computer server. That is not the case with private Cloud Computing. This leaves companies with the question which category of Cloud Computing to choose. There are hardly any scientific publications on this matter.

1.1 Research question

This leads to the following research question:

Which strategy must be followed in order to make the right choice to place a part of the business process in a cloud?

The main objective of this research is to come up with a strategy using business rules that will lead companies when they are placing business processes into a cloud. Companies use multiple business processes in there company. In the case of private Cloud Computing the whole business processes will be taken over by one company as stated earlier. With public Cloud Computing this does not have to be the case. The choice between the two options is not that clear. It can vary between business processes. This needs to be considerate when applying the different techniques. First background information is provided about Cloud Computing and business process. The next step is to explain how the problem will be solved

with the Cloud Computing solution. The last step is to apply the risk tree format on the business rules. The business rules are the outcome of the risk analysis and will form the strategy.

2 Process and Strategy

In this section business processes, Cloud Computing and Cloud Computing strategy will be defined. First, the business process approaches will be discused. There are two types of approaches that can be used and they are called *process* and *data*. With the process approach the attention lays solely on the processes, this is in line with the current research. The data approach focuses on the data that is used within a company. The difference is that the process approach gives a overview of the processes and the data approach gives a overview of the data. In the current study the process approach is used in order a decision whehther to place a business processes in a cloud. Processes can help to establish a strategy for a company which is the goal of this research. When the data approach would have been used to come up with a strategy the result would be very messy and would not give the complete answer to my research question [**?**]. Processes are great to come up with a strategy [**?**]. Therefore, the process approach is chosen over the data approach in this research.

2.1 Determining a business process

Since business processes are being used within the company, they must be examined whether they can fit within a cloud. It is important to define what a business processes is, therefore a definition of a process will be given. According to Edward Deming, a influential person in process engineering, a process[**?**]:

A process is a group of related tasks that create value.

A process consists of tasks and contribute by creating value. Now, a defintion will be given for business process. Davenport, a person that has influence in the field of bussiness processes, has given the following definition of a business process[**?**]:

A business process or business method is a collection of related, structured activities or tasks that produce a specific service or product (serve a particular goal) for a particular customers or customers.

In order for a process to be a business process it has to be a collection of structured activities or tasks and those activities or tasks have to produce a specific service or product for customers. These are measures to determine whether a process can be called a business process. The goal of this research is to give a wellfounded answer to the question which type of cloud to choose. To reach this goal a risk analysis technique will be used. The risk analysis technique is a quantitative technique. This techinque has been chosen because it does not necessitate the usage of categories with vague criteria[**?**]. The technique identifies the threats and vulnerabillities based on the risks for all business processes. Threats are the

potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.[**?**] And a risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence.[**?**]

2.2 Describing a strategy

A part of this research focuses on formulating a strategy. Strategy is the pattern of decisions in a company that determines and reveals its objectives, purposes or goals produces the principal policies and plans for achieving those goals, and defines the range of business the company is to pursue. [**?**]. It differs from a vision, what a company adds to the market. Strategy focuses on defining a goal or an objective which a company is trying to achieve.

This research uses a risk model to determine the risks of the processes that are in scope. The outcome is an overview of the risks of the threats. In order to determine how the business rules will be used an risk tree format is introduced. This format creates an overview of the vulnerabilities and the rules that counter the risks for each threat. The highest level is the threat itself, one level below are the vulnerabilities and below that are the action plans to counter the vulnerabilities.

2.3 Cloud Computing

Cloud Computing refers to the services that are provided to a customer over the internet, involving the provision of hardware and software from a datacenter [**?**]. There are many definitions of Cloud Computing, which are not always clear because the terms utility computing and grid computing also need to be explained. It is important to understand that Cloud Computing goes a lot further then grid and utility computing. Grid computing is the combination of computer resources from multiple administrative domains for a common goal[**?**] and utility computing is a service provisioning model in which a service provider makes computing resources and infrastructure management available to the customer as needed, and charges them for specific usage rather than a flat rate [**?**]. The difference between grid computing and Cloud Computing is that Cloud Computing provides more than a just computer resource. Within Cloud Computing all of the layers are being used and with grid computing only the computing power itself that is used. The difference between Cloud Computing and Utility computing is much smaller than the difference between Cloud Computing and grid computing. Cloud Computing can be seen as an evolved state of utility computing. Private Cloud Computing entails that a cloud provider will provided the business process for one company and not multiple. The different layers can not be distinguished that easily. But for public Cloud Computing this is not a problem.

The layers of a public cloud can be divided into:

- SAAS: With Software As A Service, the application is completely under control of the cloud provider. The user can connect to the cloud and software is provided to the consumer in the form of a service.
- DAAS: With Data As A Service, this layer will take care of the data storage in the cloud and will be managed by the cloud provider.
- PAAS: Platform As A Service. In this layer the infrastructure has been taken over by the cloud provider. This means that the customer does not manage the underling cloud infrastructure, network, environment and configurations.
- IAAS: Infrastructure As A Service. In this layer the framework and the infrastructure are managed by the cloud provider and the customer does not have to worry about which hardware to use. The customer does not manage the infrastructure which includes the operation systems, network components and storage.

In short, SAAS can be applied to services, DAAS can be applied to storage, PAAS can be applied to platforms and IAAS can be applied to infrastructure the a company needs. The different layers can be clearly seen within public cloud but in a private cloud these difference are not that clear. The layers can have some overlap. That is important to understand the differences.

2.4 The issues of Cloud Computing

There are also a lot of skeptic people that are against the use of Cloud Computing. According to them the security and redundancy aspect play a big roll. An example: a cloud provider is just a single company and that is why it can be seen as a "Single point of failure". When a cloud provider cannot be reached, for whatever reason, every customer of that cloud provider has a problem. Also a lot of hacking attempts are performed on public clouds[**?**]. A large percentage of the hack attemps have the goal to steal data from a company. [**?**] There is a list with all issues of Cloud Computing. The list below is just a small fraction of the original list[**?**] [**?**] [**?**]:

1. Open Client: a cloud provider can have a standard platform that is not compatible with other platforms. Access between the platforms is diffcult and a workaround must be made just to make the communication possible. An open client automaticly solves this problem. So the issue is that the access must not depend on the platforms or a special kind of infrastructure.
2. Management and Governance: A second issue is how cloud providers deal with the

regulation of different rules. A cloud provider can have many different customers with many different rules. The demands for risk control from the customers are high for the management of the cloud provider. The issue here is that it is very difficult to control risks of a other company.

3. Service level agreement(SLA): A service level agreement contains an agreement with a determination of the service levels required by a customer. Although customers have different demands for a cloud provider, the required service level is always high. It can be diffcult for the cloud provider to keep the performance high for all of the customers.

4. Availability of a Service: Cloud providers provide services for multiple companies. When the cloud provider cannot be reached anymore due to a power failure or a other reason, the customers cannot use the service anymore. The issue is here that when the cloud providers not available anymore the customers cannot use their services.

5. Data Leakage: Many cloud provider use redundancy techniques to spread the data over multiple locations in multiple countries. This is cheaper for them because they use the follow the sun principle to cut down the energy bill. The follow the sun principle is a model for datacenters. Data of the customer is stored within the cloud. The datacenter is active at night to reduce the energy bill and the data of the customer is sent to active datacenter. But the cloud consists of multiple sites that can be separated over many countries. The country where the sites are in, determines the rules that apply on the data. This can cause problems because there different regulations that can apply. This can mean that the data is not always safe. The chance of data being leaked is much bigger with this approach. Allthough the spreading of data will reduce costs it increases the chance of data leakage.

6. Data Locking: The data that is used in a cloud is usually stored within the cloud. The customer does not need to worry about the data. But when the cloud provider is bankrupt or wants to switch to an other cloud provider, the data cannot be transferd. So the issue is that data can only be used within the cloud provider.

7. Data segregation: In the case of Cloud Computing many users use the same application and the data is stored on the same machine. The data of the customers is not spread. When something wrong with the data on a machine all the customers have the a problem. The issue is here that the data is not separated.

Because safety issues are a hot topic when the use of Cloud Computing is discussed, the focus will be put on those aspects. Moreover this means that the focus of this master thesis will be put whether to place a business process in a cloud. This aspact has not researched before, this means it is very interesting [**?**] and will contributed by making the right choice when it comes to this subject.

3 Model

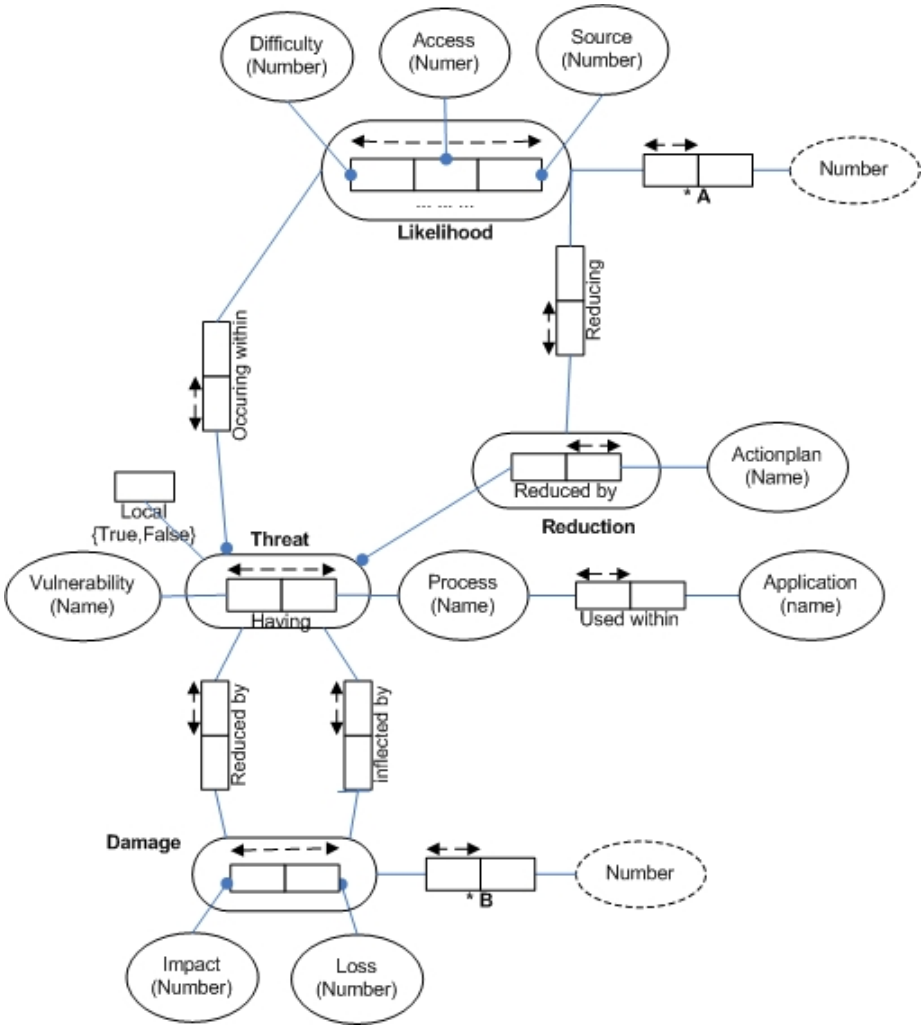

Figure 1: Overview of the theory

In this section the model that is used for the risk analysis is explained step by step. To determine the total risk of all the business processes a risk analysis will be used from Lenstra and Voss [**?**] This technique gives an accurate estimation of the total risk form all of the business processes. The technique first determines for each business processes the *risk of threat* which indicates the current risk for the business processes. This is based on the type of loss and the impact on the business processes. After that the *aggregated risk of application*

is calculated, which is a result of the combination of all the business processes. After that it is important to investigate if there are some factors that can positively influences the risk indicator. To determine the impact on the business process the *total residual risk of process* is calculated. The same information for the current IS indicator is used but now action plans are used instead of threats. The *aggregated residual risk of application* can also be calculated, with the same technique that was used for the current risk indicator. After that the risk profile is known and the bussiness rules are translated with the risk tree format into a strategy. The business rules are the action plan to counter the threat. That is short version of the technique, a detailed overview can be seen found in Figure 1.

But first it is very important to make distinction between two terms that can be applied on my research. The terms are called Security and Safety. These terms are often confused and must explained precisely. Security: measures taken to guard against espionage or sabotage, crime, attack, or escape. (webster) Safety: the condition of being safe from undergoing or causing hurt, injury, or loss. (webster) This are two clearly different terms. The difference is that security involves an attacker that wants to attack by investing time or money and gaining fame or steeling something like data. The term safety does not have this difference. Moreover, security can have more vulnerabilities that cause attack. For example when an attacker wants to steal your data, a vulnerability could be your backups. In order for them to steal your data from the backup, they could exploit another vulnerability. They could crash the system so that the backup tapes are needed. This has to with security and not with safety.

That being said, looking at my model it is more safety orientated. The vulnerabilities are depending on each other and the attacker is not showed in the model. This is problem because the aim of this research is security and not safety. This important issue, can needs more research. That is why it must be further researched. The term threat is used a lot in this research. It must not be confused. The term implicates a safety issue and not a security issue.

A suggestion could be to improve the model, that the attacker must be added to the model. Also the gain of the attacker must be added and the investments. The vulnerabilities must be able to independ on each other. This will start transforming the model from safety oriented to more security oriented. This will improve the model a lot but it still does not cover the whole part of security; Sometimes a hacker just wants fame and does not have to investment something. But there are more question that need to answered to improve the model.

3.1 Risk of threat

To estimate the likelihood of a threat, three subparts will be used. These are level of difficulty, access and source. The concept source consists out of two groups, one is named internal and the other is named external. Internal implicates that the threat will come from inside the company and external implices that threat comes from outside the company. An external source has a high chance to occure because the threat occures more on cloud providers. The value of a internal source within a company is also higher because the information is more important. Because of the importance of the data the likelihood will be higher.

Access consists also out of two groups, namely local and remote. Local implicates the access the threat needs. The source indicates were it is originated from and access implicates from which source the threat starts from. The threat startes at the source. It can be local which means it is from inside the company or it can be remote which implicates that is from outside of the company. Remote access has a low value because there are less threats that can apply.

The last part is the level of difficulty which implices the needed competence to executed the technique. This part consists out of two groups named structured and technical. Structured indicates that is a complex threat. Technical indicates that are a lot of complex resources involved in this threat. Structured and technical have a low value because the likelihood of occures is low. But it is also possible that the threat is not unstructured but technical and that results in a higher value. The opposite of these groups are than of course structured and non technical. Which results into a normal value because the chance of occures is lower. The bases of the values are all based on the following literature [**?**], [**?**]. The basis has been made to apply the technique. Because the technique has a mathical approach, the explanation will be presented in mathical style. A lot of formulas will be used to explain the approach.

With the information of the type of threats it is possible to calculate the *Likelihood of occuring of threat*. In the theory of Lenstra and the Vos this is called the *current likelihood indicator*. In Figure 1 you can find the symbol A on the top right side. The current likelihood indicator is of course without any action plans and implicates the chance of occuring. The values consits out of level of difficulty, access and source. Lenstra and the Voss have derived the type of threats from a other article[**?**]. They remark that it only will give an indication until there is determined that are indicators. One name has been change to not confuse them with other terms, originally difficulty was called skill. The likelihood will be calculated with the following formula:

Likelihood of occuring of threat t
=
(Nr of Diffcult in Likelihood occuring in Threat t)
∗(Nr of Access in Likelihood occuring in Threat t)

∗(Nr of Source in Likelihood occuring in Threat t)

The threat of a business process can be indicated by calcuting the damage. This can be done by using the combination of impact and type of loss. One condition applies that damage is above 0 and below 1. The impact implicates the value of the threat when it occures. For example if all of the data is gone this is big problem, that is why the value will be high then. The type of loss indicates the impact on the assets. To give an example to lose an server or mouse is very different. That is why the value will implicated the severity of the loss. With combination of that information, *damage caused by threat t* is calculated. In the theory of Lenstra and the Voss this called the *current risk indicator with respect to the threat.* In Figure 1 you can find this indicated with the symbol B on the right bottom part of the Figure. The difference between those two is that the A part applies to the likelihood and the B part to the damage of a threat. The damage can be calculated with the following formula:

Damage caused by threat t
=
(Number of Impact in Damage inflected by Threat t)
∗(Number of Loss in Damage inflected by Threat t)

So now we have calculated the likelihood and the damage of a threat. The next step is to calculating the risk of that threat. This can be done by multiplying the damage times the likelihood. Next we are going to take a look at the threats of a process.

Risk of threat t
=
(Likelihood of occuring of threat t)∗(Damage caused by threat t)

After the last step only the value of one the threats is known and the risk of the combination of the threat must be known. This all based on the information of the previous steps. Next the *total risk of process p* will be calculated for all of the business procesess. In the theory of Lenstra and the Vos this is called the *current IS risk indicator of process.*

Total risk of process p
=
Sum t: Threat of process p: Risk of threat t

Now the first part of the risk analysis is almost done only the *Aggregated risk of application a* has to be calculated. In the theory of Lenstra and the Vos this was called the *current aggregated IS risk indicator.* Now we have the threat for one business process and the goal is to calculated the total risk of all the procesess. This is the combination of all the threats for all of the business procesess. With that combination you will have the total risk of the

business process without any action plans to counter the threat.

Aggregated risk of application a
=
Sum p: Process used in application a : Total risk of process p

3.2 Residual risk of threat t

Of course there are some circumstances that can help to reduce the risk. An example can be an action plan that will counter the risk. If the threat is a room is not secured you can place on lock on it. Placing a local is called an action plan to counter the threat. First the *effect actionplan a* must be calculated. In the theory of Lensta and the Voss this is called the *residual likelihood indicator* This works as the same principle as the *likelihood of threat t*. For each type of threat (source, access and difficulty) the user enters a value that corresponds with the residual risk. The value that has been entered must be between 0 and 1. The action plans will be based on the industry standard. The action plans is based on a industry standard to create a more transparent overview for other parties that can be involved. In the case of information security that usually means the ISO27002 standard or in the case the food industry this can be the CGXP standard. The term reducation stands for *Likelihood reduced by reducation of an actionplan a*. This term is used to shorten the sentence.

Effect actionplan a
=
(Nr of Diffcult Redaction a)
∗(Nr of Access Redaction a)
∗(Nr of Source Redaction a)

After the residual IS risk indicator of the process is calculated. This includes the *damage reduced by threat t*. In the theory of Lenstra and the Voss this called the *residual IS risk indicator with respect to the threat*. That will indicated the reaming damage that threat can have on the processes. The formula is as followed:

Damage reduced by threat t
=
(Number of Impact in Damage reduced by Threat t)
∗(Number of Loss in Damage reduced by Threat t)

Again the likelihood and damage can be calculated for the action plans. The risk of the threat can be determined with the same principal as before. Damage multiplied with likelihood will

results into to the Residual risk of threat. In the theory of Lenstra and the Voss this is called the Residual risk of threat t

Residual risk of threat t
=
(Effect actionplan a)∗(Damage reduced by threat t)

After the *total residual risk of process p* is calculated. In the theory of Lenstra and the Vos this is called the *residual risk indicator of the process*. The same principle of the current risk indicator of the process will be used but now for the residual risk. The formula for this:

Total residual risk of process p
=
Sum t: Threat of process p: Residual risk of threat t

The new risk indicator with the reduced risk can be summed up for the all the business process. The value will indicate the reaming risk after the action plans have taking effect. This called the *aggregated residual risk of application a*. In the theory of Lensta and the Vos this is called the *residual aggregated IS risk indicator*. This can be done with the following formula.

Aggregated residual risk of application a
=
Sum p: Process used in application a : Total residual risk of process p

After determining the *aggregated residual risk of application a*, we now know the residual risk. But a lot of action plans can be used. Which of those plans have the best effect on a process? In other words, when should we use an action plan. Which one will have the best results on a threat. The formula below we determine that.

Best effort p
=
Min(Effect actionplan (reducing process p))

But there are more than one proceses that are used. That results into the question, which of the action plans will result into the best of plan for the processes? The formula below will indicate the optimale plan for process p. The optimal plan will be selected with this formula.

Optimale plan for process p
=
Actionplan a: Effect actionplan a = Best effort p

3.3 Classification

Now we have calculated the current and residual risk indicators. With this information we can determine whether to place a business process into a cloud. By classifying it we can compute a percentage and determine the risk profile. If the percentage is high, that will mean there is high risk when using a cloud provider. It can be calculate with the following formula.

$$\textbf{Risk} = Curtriskp \; - \; Restriskp * 100$$

After classification we know whether to place a business process into a cloud. Next the business rules will be analyzed with a the risk tree format. Each rule for each threat can be split up in smaller pieces. The rules will be used to determine the strategy for a company.

4 Business rules approach

In this section the business rules approach is explained, it includes severy aspects. First the use business rules will be explained. Business rules are the rules that form the strategy for your company. As stated earlier in Section 2 about bussines rules, the rules constrain and enforce safety to ensure that your system or process works the way you want it to. The business rules can be found in the Section 3 model and are shown in Figure 1. In that section they are called action plans. The residual damage and likelihood can be calculated just like it is stated in the model. Damage is the combination of the concept of *impact* times the concept of *type of loss*. *Likelihood* consists of the concepts *Difficulty* times *Access* and *Source*. That are the basics that are also applied within the risk tree format. The risk tree format is derived from the risk tree format of Bruce schneider[**?**]. In the orginal form it was a way to model security issues. Because the model in Section 3 model is more safety oriented the name risk tree has been chosen. The business rules consist of rules that counter a threat, which is also a concept in the model. An example of a action plan will be given from the ISO270002 (standard).

> A.7.1.1 Inventory of assets Control All assets shall be clearly identified and an inventory of all important assets shall be drawn up and maintained.

There are two kinds of rules, elementary rules and combined rules. In the subsection combined approach you can find the operator *AND*. This is an example of a combined rule. Elementary rules are rules that can not be split up. An example of an elementary rule is: *The room must be secured*. The operators that can be used are AND, OR or NOT. When these rules are used in a senctence that indicates that rule is a combined rule.

An example of a combined rule is: *The room must be secured and can only be used by authorized staff*. The AND operator indicates that it is a combination rule. This means that the rule will be split up into two elementary rules. This makes the use of rules easier.

4.1 Global approach

In Section business rules we made a clear distinction between elementary rules and combined rules. The global approach can be applied on the elementary rules. Therefore we are going to use a *risk tree*. An *risk tree* consists of a threat, vulnerabilities are countered by guardians. In Figure 2 it is called worst scenario, node C is the threat; edges $V_1, \ldots, V_n$ are the related vulnerabilities and protecting guardians are $B_1, \ldots, B_n$ for the vulnerabilities. The risk that is guarded by an interior node is delegated to the underlying guarding nodes. A leaf of an risk tree can be seen as an independent guardian. Without the support of a delegated the

threats countered by the interior node are not reduced. This is referred to as the *worst case* scenario for that node.

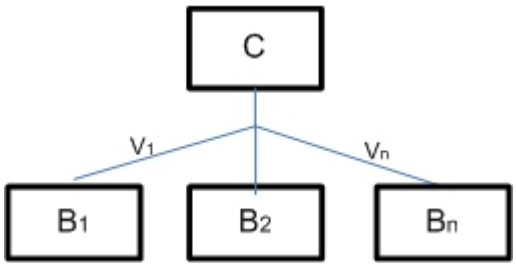

Figure 2: Worst case scenario

For leave nodes there is no difference made between the worst case scenario and the *protected* scenario since the leaf node have no delegates. For the interior nodes the realistic scenario will be an improvement of the worst case scenario. We will introduce calculation rules to calculate the residual risk in the protected scenario. The residual risk is calculated using the likelihood and the damage of the vulnerability. The likelihood of a vulnerability indicates the chance of occurring as explained in subsection 3.1 current risk indicator. In Figure 3 called the realistic scenario; node C has vulnerability which is reduced by a guardian with a likelihood and a damage.

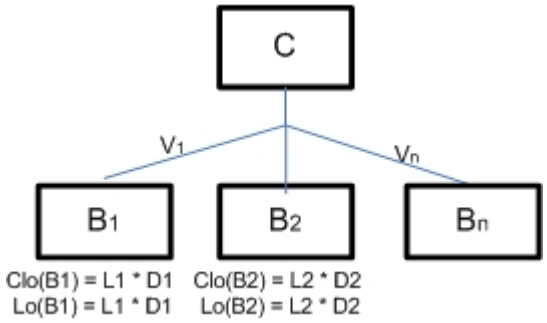

Figure 3: Worst case scenario

Likelihood is calculated with the combination of the source (SO_j) * difficulty (SK_j) * access (AC_j). That will lead to a number between 0 and 1. In this formula source indicates the place where the threat originated from, access indicates what kind of access is needed when

the threat occures and level of difficulty will indicate how difficult the threat is. Next the damage of a threat must be calculated.

Damage indicates the impact when the vulnerability occurs as described in subsection 3.1 current risk indicator. Damage D_i consists of the type of loss TP_j * impact IM_j. The type of loss will be indicated by the loss of the asset(anything that has value to the company [**?**]) in question. Impact indicates the damage that is done by the vulnerability. A concept can be applied on two types of clouds Local and Cloud. It is important to note that not all of the vulneribilties will apply on both of the type of cloud. Some vulnerbilities are more related to public Cloud Computing than to private Cloud Computing.

Local:	**Cloud:**
$\text{Local}(\text{L}_j) = SO_j * AC_j * SK_j$	$\text{Cloud}(\text{L}_j) = SO_j * AC_j * SK_j$
$\text{Local}(\text{D}_i) = TL_p * I_p$	$\text{Cloud}(\text{D}_i) = TL_p * I_p$
$\text{Local}(\text{B}_i) = L_j * D_j$	$\text{Cloud}(\text{B}_i) = L_j * D_j$

The threat risk is a combination of B_1 which are related to C_1. In Figure 4 below there are two vulnerability risks determined.

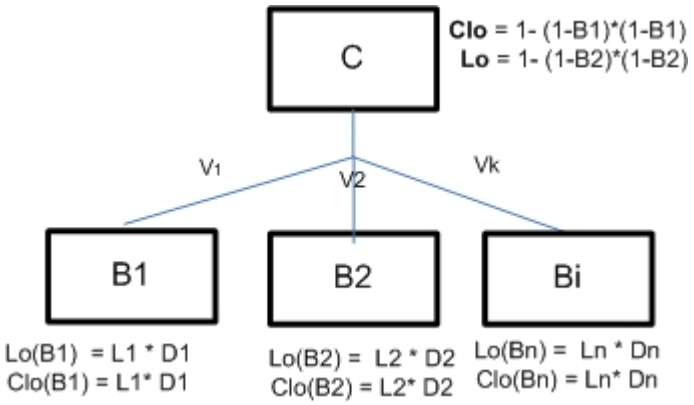

Figure 4: Calculation of residual risk

In general the residual threat risk is calculated following:

$\text{Local}(c) = 1 - \pi_{i=1}^{n}$ (1-local(Bi))

$\text{Cloud}(c) = 1 - \pi_{i=1}^{n}$ (1-cloud(Bi))

To explain the formula above an example will be used. Take for example three lights that are parallel lined to together. In order to be dark the all must be broke. So for the chance for

light for one of them is equal to the chance of dark minus 1. The combination of all three of them is chance of being light. That leads use to the formula 1-(1-light1)*(1-light2)*(1-light3).

When the threat risk is 0, this will lead to the best case scenario. When the risk is higher than 0, this will lead into the realistic scenario. However, a guardian can be a new vulnerability. This is called a *new* scenario. See for a example Figure 4 called a new case. When B_i has a vulnerability that is reduced by A1 and I, the guardian A_1 can be calculated just like when we determined the likelihood and the damage. The next step is to calculate the residual risk of cloud and for local for the threat.

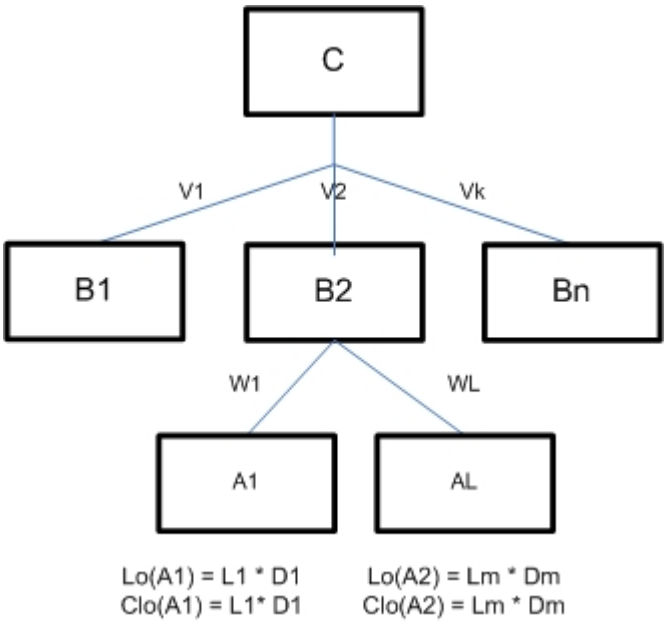

Figure 5: New case

According to the rule that each new concept introduces a new risk, a new scenario can be formulated. This process will continue until the residual risk is 0 or until there are no guardians to counter the vulnerability or the risk is accepted by management. The risk tree can also be applied to more one threat, and one threat can be applied to more than processes. All the threats for all of the processes must be determined to calculate the total risk. This has been described in Section 3 model.

4.1.1 Margin of error

The numbers that are used to calculate the risk need to be based on the opinion of a domain expert. The numbers can have a deviation. That is why a margin of error can be added to improve the precision of the indication of a domain expert. By adding a δ value(margin of error) to each guardian the margin of error is incorporated in the formula. The basic formula is expanded to:

$$\text{Local}(c) = 1 - (\pi_{i=1}^{n}(1 - \text{L}(Bi) + \delta_i)$$

The explanation of the formula and how the formula is build up can be found in the Section Formula in the appendix. This means that for each guardian of vulnerability a margin of error could be added. The domain expert can added a numeric value to the formula. It does not have to be added if it is not necessary. It does not matter if there is a 0 that is included in the formula because they are added with together. Because the formula is quite technical of his nature a simple formula is presented. In the example in Section Formula there are three guardians that have a margin of error. That can be expanded if needed.

$$\frac{Error}{Value} = (\frac{\delta_1}{A_1} + \frac{\delta_2}{A_2} + \frac{\delta_3}{A_3})$$

4.2 Combination approach

In the previous section we have looked at the elementary rules and explained the base of the business rules approach. In this Section, combined rules will be explained. To demonstrate the complete technique, a larger example will be given. This example also consists of rules, but this can be split up into elementary rules. The topic of the example is Cloud Computing, because it is the main topic in this research. Let us presume that the threat is data locking and call this C1. Data locking could cause big problems for cloud computing. Because there are no standards determined, reusability is very low. This can become a safety issue, like when the cloud provider is bankrupt or the data is gone. That will mean that the data cannot be used outside of the cloud. C1 has the following vulnerabilities:

- V1: Cloud provider goes bankrupt; the credit of the cloud provider plays a big part here. If the provider is bankrupt that data can not be transferred.
- V2: Local data are lost; the data which are used locally are gone. This means that data outside of the cloud need to be obtained. That is of course a different standard.
- V3: Application has another data type, the local standard and the cloud standard is different so application that are used locally that use the data for the cloud.

Using the business rules approach will lead to the risk tree format with some action plans. The explanation of the values will be described below. The focus is not on selecting the business rules, but mainly on applying them in the right manner.

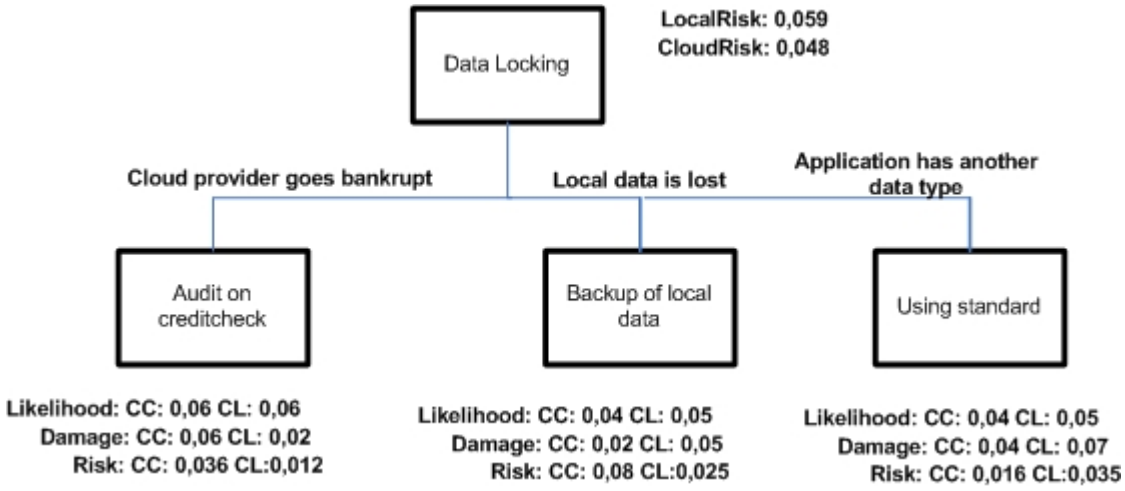

Figure 6: Present Situation

Of course there will be guardians to counter the vulnerabilities. The action plans are the business rules that are split up into the elementary rules. These rules are based a standard, But that is not the focus when we are using the risk tree format.

- B1: Audit on Credit check, check the sustainability of the cloud provider. This can be done by checking the annual report of the cloud provider.
- B2: Backup of local data, make a backup of the local data and store it on different places. The rule looks like A.10.5.1 Information back-up from the ISO 270001 standard. The rule is about software and backup. The rule can be split up because the software part does not have to be a part of the rule.
- B3: Using standards for applications to insure usability. A rule that looks like this one is the A.15.2.1 Compliance with security policies and standards from the ISO 270001 standard. By splitting it up, the policy and standard can be separated.

The guardians are reduced the leaves of the tree and the residual risk can be calculated. The likelihood and the damage can be determined based on the indicators. In the case of likelihood is the combination of Source (External, Local), Difficulty ((un)Structured, (un)Technical) and Access(remote, local). In the case of damage is the combination of type of loss and impact.

Local:	**Cloud:**
Source of V1: External = 0.4	Source of V1: External: 0.4
Difficulty of V1: Structured technical = 0.3	Difficulty of V1: Structured techincal:0.3
Access of V1: Local= 0.5	Access of V1: Local: 0.5
Likelihood of V1: 0.4 * 0.3 * 0.5 = 0.06	Likelihood of V1: 0.4 * 0.3 * 0.5 = 0.06

An audit can be done by a third party outside the company. This external party checks the creditability. To perform the audit check, certain skills are needed. These difficulties are structured and technical, they should be capable of planning and the technique needed to do this should be available. The likelihood that will occur is calculated using a combination of the three indicators (see formula at likelihood v1) and results into the value 0.06. This value entails that there is not any difference found. That means that it does not matter if it is in the cloud or not.

Likelihood of V2:

Cloud:	**Local:**
Source of V2, External: 0.4	Source of V2, External: 0.5
Difficulty of V2, Structured untechnical: 0.2	Difficulty of V2, Structured u technical: 0.2
Access of V2, Remote: 0.4	Access of V2, Local: 0.5
Likelihood of V2, 0.4 * 0.2 * 0.4 = 0,032	Likelihood of V2: 0.4 * 0.2 * 0.5 = 0.05

The action plan has to do with the backup that is made for the users of a cloud. The action plan uses a source from an external cloud, because the action plan has no control over the data coming from customers. And for the customers that entails local computing. The levels of difficulty that are needed are the same for both external and cloud part; structured but easy because it is not technical. It is structured because it is done regularly. The cloud provider has remote access, as the operations on the cloud are not done locally. The following formula is set up, leading to the likelihood of 0.05 for the local part and the cloud part it is 0.32.

Likelihood of V3:

Cloud:	**Local:**
Source of V3, Internal: 0.4	Source of V3, External: 0.5
Difficulty of V3, structured technical: 0.2	Difficulty of V3, Structured technical: 0.3
Access of V3, remote: 0.5	Access of V3, remote: 0.5
Likelihood of V3, 0.4 * 0.2 * 0.5 = 0.04	Likelihood of V3: 0.5 * 0.2 * 0.5 = 0.05

The standard technique has different effects on the cloud provider and the user. For the user, the source is external and standardized. For the cloud provider, the source is local. The levels of difficulty used that are used for the cloud are structured and technical because they have to plan and implement the standard to the cloud. The users do not have to have any difficulty, they only need to make use of it. The access to the cloud is the same for both parties because the standard is taken from others, such as the w3c company. The following

formulate is set up, leading to the likelihood of 0.04 for the cloud part and for the local part it is 0.05.

Damage of V1:

Cloud:	**Local:**
Type loss of V1, 0.1	Type loss of V1 0.4
Impact of V1: 0.2	Impact of V1: 0.2
Damage of V1: 0.06	Damage of V1: 0.02

The damage that can be seen in the Section model, consist of two indicators; type of loss and impact. The type of loss is credit check which is important for users of the cloud but it is not important for the cloud provider. The impact of the threat for both the cloud provider and the users is small. This is based in the indicators damage and likelihood, which show a value of 0.02 for the local part and for the cloud part it is 0.06. The outcome of this is the following damage:

Damage of B2:

Cloud:	**Local:**
Type loss of B2, 0.1	Type loss of V2 0.2
Impact of V2: 0.2	Impact of V2: 0.3
Damage of V2: 0.02	Damage of V2: 0.05

The type of loss when the data is locked from the cloud provider and local is for the user is the same; the damage is significant. The same applies for the impact, although it is worse for the user because they cannot do anything. This is why the value of 0.02 is higher there, the higher value entails 0.05.

Damage of B3:

Cloud:	**Local:**
Type loss of B3, 0.2	Type loss of B3 0.3
Impact of B3: 0.2	Impact of B3: 0.4
Damage of B3: 0.04	Damage of B3: 0.07

The type of loss for not using the standard is the cause for this threat data locked in. This value is not high for the user because it concerns the cloud provider. That is why the value is lower. The impact it has on a user is higher, because they have a problem when the cloud provider is not using that to reduce the impact it has on a user. This is why the value of 0.04 is higher there, the higher value entails 0.07.

Now we can calculate the risk for the action plans B1, B2 and B3. This can be done by combination of the damage values with the likelihood values. This results into an action plan of B1 local (0.24), Cloud (0.18), B2 Local (0.08), Cloud (0.31), B3: local (0.16) and cloud

(0.35). The threat risk is calculated using the following formula: 1-(1-V1)*(1-V2)*(1-V3). This results into local (0.41) and cloud (0.63).

But these indicators do not have a margin of error. An example could be that a margin of error for B1 is 0,02. That will imply that the δ of B1 is 0.02. This is explained in Section Formula. According to that formula this means that 0,02 will be divided by L(Bi)= 0.24 and C(Bi)= 0.18. That results into L(0,083) and C(0,111). The threat risk with a margin of error results into Local(0.29)and Cloud(0.60)

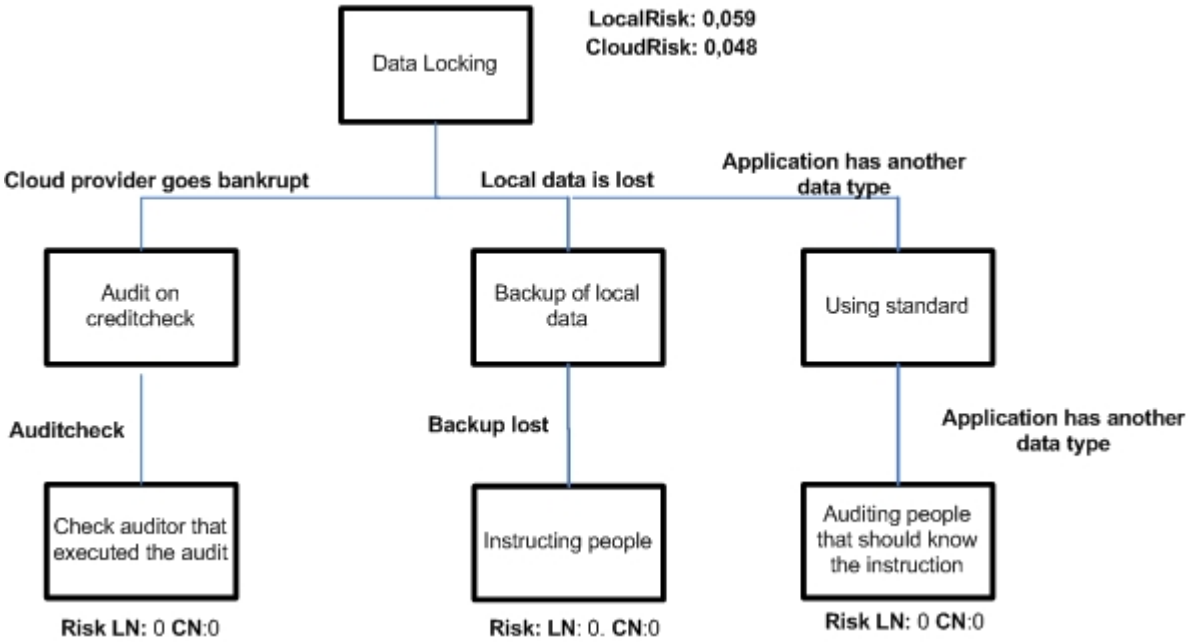

Figure 7: New Situation

Now we have done the first step and the next step is as you know is to apply the basic rule. The next part can be seeing in the example *New* situation. The basic rule is that a guardian introduces a new threat risk. In Figure new situation, you can see that the threat risk will came to zero. The new vulnerabilities are V1 *audit check*, V2 *backup is lost* and V3 *standards aren not used*. The new action plans to counter this are A1 *check auditor that executed the audit*, A2 *instructing people* and A3 *auditing people that should know the instruction*.

The likelihood and the damage are calculated as the same manner as before. This results in to the following risks for B1, B2 and B3. There is no risk anymore because the B1, B2 and B3 neutralize the new vulnerability. There is no further research not needed because V1, V2 and V3 result into 0. This risk tree is closed now and the new risk results into zero.

4.3 Final thoughts

Using the business rules approach it is simple to determine which rules will form your strategy. Without using it is just selecting them out of the risk analysis without looking at them properly. By making a distinction between elementary and combined rules the threat can be counter with a more formal way. The threat is always on top of the tree and the leaves contain the vulnerabilities. The business rules that counter the vulnerability will be split up into multiple rules. Each new action plan will introduces new threat and must be look at. That processes will continue until the threat is zero or the management will accept that risk. When appling the vulnerbilities it is important to notice that not all of them can be applied to both the concepts of cloud and local.

The numbers that are chosen by the domain expert are between 0 and 1. That is an important condition that needs to be applied when numbers are chosen. Because this technique is new, there is not a lot data available to determine a high value or a low value. This can be improved by evaluating the data when the technique has been applied multiple times. With more data the estimation can be more accurate. To give the domain expert an indication, some categories can be used. The categories are suggested by Lenstra and the Voss until there is more data available. A number between >= 0,6 can be used when it is a threat with a high category. The number < 0,2 can be used when the threat is low and in the case of medium it can be between those two values. The values are just indication as clearly stated in there article to give a reference for the domain expert. The values can be more exact when there is more data available.

Of course some rules are more important than others. That part is worth the investigated more but then with more data you can be more specfic and apply it on more situations. Also there are more operators that can be used. Some rules can imply dependencies, but there is not enough data availability to come with an answer to that part. To sum it all up, with more data it is worth to investigated.

5 Conclusion

In this research we have determined whether to place a business process into a cloud. A strategy will determine whether to place the business processes in the cloud. The strategy formulated with the use of business rules. With the model a risk analysis could be performed to determine if the business process could be placed into the cloud. Business rules are the action plans that counter a vulnerability of a threat. The business rules can be place in a risk analysis format to determine whether they should be used for the strategy.

With this technique business rules can be selected for the right strategy. Even with different scenarios like "Worst case" or "Best case" this can be done. With the risk tree format we have seen that the complicated rules can be split up into smaller pieces to counter the threats. An action plan can be stripped down and can be examined in detail. The new technique is worth to investigate. It can be optimized and it can be applied on practical problems. The combination of different operators like AND or OR can also be used and dependencies can be showed in the risk tree format.

Other important issue is that there is a difference between the term safety and security as has been discussed in Section 3 model. The model we have used is more safety oriented model and must be altered to be a more security oriented model. In a further research the most important adjustment could be adding an attacker in the model, adding the gain and investment of the attacker and the last adjustment is that the vulnerabilities must not depend on each other.

References

[1] J. Archer and A. Boehm. Security guidance for critical areas of focus in cloud computing. *Cloud Security Alliance*, 2009.

[2] M. Armbrust and A. Fox. Above the clouds: A berkeley view of cloud computing. *Berkeley*, pages 1–28, Feb 2009.

[3] A. Arundel and H. Hollanders. Innovation strengths and weaknesses. *Enterprise Directorate-General, European Commission*, 2005.

[4] F. M. Aymerich and G. Fenu. An approach to a cloud computing network. *Department of Computer Science, University of Cagliari, Italy*, 2008.

[5] T. Davenport. Process innovation: Reengineering work through information technology. *Harvard Business School Press Boston*, 1993.

[6] N. J. Foss. Resources firms and strategies. *Oxford*, 2003.

[7] I. Foster and C. Kesselman. The anatomy of the grid. *Supercomputer Applications*, 2001.

[8] M. Hammer. The reengineering revolution. *HarperBusiness*, 1995.

[9] ISO. Concepts and models for information and communications technology security management. *International Standards for Business*, 2004.

[10] B. R. Kandukuri and R. Paturi. Cloud security issues. *IEEE International Conference on Services Computing*, 2009.

[11] A. Langely. Strategies for theorizing from process data. *Universite du Quebec a Montreal*, 1999.

[12] A. Lenstra and T. Voss. Information security risk assessment, aggregation, and mitigation. *Technische Universiteit Eindhoven*, 2004.

[13] K. D. Loch and C. Houston. Threats to information system today's reality, yesterday's understanding. *MIS Quaterly*, 1992.

[14] P. Mell and T. Granc. The nist definition of cloud computing. *National Institute of Standards and Technology, Information Technology Laboratory*, 2009.

[15] L. Mohr. Explaning organizational behavior. *San Francisco Jossey-Bass*, 1982.

[16] M. A. Rappa. The utility business model and the future of computing services. *IBM Systems Journal*, 2004.

[17] B. Schneier. Attack trees. *Dr. Dobb's journal*, 1999.

[18] G. Stoneburner and A. Goguen. Risk management guide for information technology systems. *National Institue of Standards and Technology*, 2002.

[19] D. van Beek. De intelligente organisatie. *Tutein Nolthenius Den Bosch*, 2006.

[20] L. M. Vaquero and L. Rodero-Merino. A break in the clouds: Towards a cloud definition. *Telefonica Investigacion y Desarrollo and SAP Research Madrid Spain*, 2009.

[21] A. T. Velte. Cloud computing a practical approach. *Mc Graw Hill New York*, 2010.

[22] M. E. Whitman. Threats to information security. *Communications of the acm*, 2003.

[23] L. Zahn and T. Dineen. Network computing architecture. *Prentice Hall Englewood Cliffs*, 1990.

6 Appendix

This section is not completely finished but it illustrates how the technique can be applied. In this section the solution will be validated by testing it on a real life situation. The electronic health dossier is the subject and is known as the EPD. This subject has been chosen because this is an information system that is used within hospitals. This means it has to be an open system but also closed system because of the very important data it the system contains. The information is based on the interviews with an expert that is active in this area of expertise. With this useful information the theory has been tested.

6.1 What is the EPD

EPD is a way for medical instances to exchange medical data. The basic idea is to improve cooperation between general practitioners, hospitals and doctors. In the year 2009 hospitals voluntary added them to this idea. The vision of this idea is that it will improve a lot medical issues. Some examples are, sharing the information with another doctor without any problems because the doctor can request your medical history and our medicine usage is known at the pharmacy, doctors and specialists.

A lot of definitions exist of the Electronic Patient Health Record, but what does it mean? For example does this mean that it contains medical records, blood values, lab results and also medical insurance data? And is it possible to read or alter data in this file? This is not clear defined.

6.2 The kind of EPD generation

Because the term EPD is not clear it be will referred to as a concept. To makes it more complicated, different phases will be added to the concept. The concept is now called EPD consists of phases. These phases are called be Gartner generations. The generations most medical instances are in is generation 1. That is the reason to take a closer look at the first generation. This is definition of Gartner.

Informative EPD, this generation is only for looking into medical data. First generation implementation is almost realized in the Netherlands. These systems lead to better availability of patient data in a hospital, but are incomplete and not user friendly. Gartner 2009

The definition of Gartner will be used when refering to the concept EPD. This means that it only contains medical history of the patient and medicine usage and nothing more.

6.3 Business Process

There is more than one option that can be chosen to determine if a business process can be placed in a cloud[**?**]. The most common and used are the data or the process approach [**?**]. Data is a bottom up approach and process is a top down approach. The idea of this research is to come up with a strategy. In the definition of a business process it was clearly stated that the process had to serve a goal. This goal can be strategy so therefore the choice has been made for the process approach.

Because of the fact that generally speaking only the first generation is used, not all the process that are in a hospital are interesting. The processes are not yet in development for the concept EPD. There a lot of processes that can be selected such as registering a patient, performing medical examination, authenticate DBC but these processes are not active. That is why the choice has been made for the following process:

> Intake, the patient is medically examined to determine a basis health situation.

6.4 Solution in terms of the EPD

For each business process the risk needs to be calculated which is based on all of the threats. This mentioned in Section model. In order to get to the aggregated risk first the *Likelihood of occuring of threat t* will be calculated. Next the impact on the business process will be calculated. This is done for each threat whether involves the use a cloud. Each threat that can have a negatively effect will be analyzed.

Intake
One of the threats that have an influence on the business process is data leakage. This refers to the loss of data out of the system. Information can be spread over multiple machine, this means it can easily disappear.

To calculate the risk a couple of steps are needed. The first step is to calculate the likelihood of the threat of the business process. There are two group namely, cloud and without cloud. The likelihood is as you know a combination of source, access and level of difficulty. The data leakage has effect in the cloud. This means it is internal and is of cours the threat is local because the threat is from inside the cloud. The level of difficulty is not so hard because it just finding the leak, that is not structured or technical. By lookup the value this results into a vulnerability risk of 0,04 for inside the cloud. Because the vulnerability is within the cloud the non cloud part is external and the access is of course then remote but the level of difficulty stays the same. The results into value for local 0,02. It is easy to calculate the vulnerability risk and it is all based on the formula. The formula in the orginal from was

about cloud and local. Now it is called Likelihood of occuring of threat t instead of Pcloud or Plocal. The following formulate is set up based on the information above about likelihood:

Likelihood(Cloud) of occuring of threat t = Source(0.02) * Access(0.02) * Difficulty(0.01)
Likelihood(Local) of occuring of threat t = Source(0.01) * Access(0.02) * Difficulty(0.01)

The same can be done for another vulnerability that can play a role when dealing with the concept EPD. Availability of a service is a service of cloud provider is not available. When this occurs the service cannot be used. This step is calculated with the same technique as before. Of course the values that have been entered are different because it is a different threat. So we are going take a look at part with the cloud and without the cloud.

With a cloud the vulnerability is external so the source will be also external. The access is remote because the vulnerability comes from outside. To exploit this vulnerability is not that hard but it needs some planning and preparation. That is why the level of difficulty is structured but not technical. Local computing has basically the same situation, it is external and the access is remote the level of difficulty is structured but non technical. The reasons are the same there is not a big difference between in the group. This leads to following cloud value: 0,12 and for local it is 0,09.
Likelihood(Cloud) of occuring of threat t = Source(0.03) * Access(0.04) * Difficulty(0.01)
Likelihood(Local) of occuring of threat t = Source(0.03) * Access(0.03) * Difficulty(0.01)

6.4.1 Risk of threat

With the information from the likelihood indicator the *risk of threat t* can be created. This will be done for all the threats that are active on the business process. The local or the cloud threat is multiplied with the likelihood which indicates the risk of threat t. The local or the cloud threat exists out of the impact times the type of loss. As explained earlier in the section model. In the orginal theory "Risk of threat t" was called Rcur(p,t).

Risk(Local) of threat t = Damage(0.64) * Likelihood(0.04)

The impact of this threat is high because the loss of data for a cloud company is big issue. A lot of critics of Cloud Computing use this as their main argument. And the type of loss is also high because the loss data is big deal for a company. That is why this is also high.

Risk(Cloud) of threat t = Damage(0.32) * Likelihood(0.02)

For the local company it is quite another story. There data is less important when you compare this with the cloud provider. This can be seen in the safety issues that the cloud providers encounter. This means that the type of loss is lower but the impact stays the same. The loss of data stays a very important issue.

The other threat availability of a service will be calculated with the same technique as the previous section. First the cloud part will be calculated and after that the local part will be calculated.

Risk(Local) of threat t = Damage(0.70) * Likelihood(0.12)

This threat has a big impact on the process intake. When this processes cannot be used the whole system is down and patients can not be helped in the hospital. The impact is very high when it comes to this threat. The type of loss is also high because the main systems are involved. That is why it results into a high value. There is no differents between local and cloud because the damage stays the same.

Risk(Cloud) of threat t = Damage(0.70) * Likelihood(0,09)

6.4.2 Residual risk of threat

Next the total risk will be calculated for the all the business process that are involved. In this section all the threats for the business process "intake" are added together. The total the risk for all the process is. In the orginal theory this was called $\mathrm{Rcur}(p,t)$ but now it is called Total risk of process p.

Total risk of process p = $\sum_{p \in P}$ Rcur(0.440)

The residual risk of threat is divided by two because otherwise the value can be above 1 and it needs to be between 0 and 1.

6.5 Effect of actionplan

Because there are some actions that can reduce the risk, the "effect of actionplan" will be calculated. For each threat the same approach is used and applied on the threat for the business process intake. First the threat "data leakage" will be examined and after that the threat "availability of a service" will be examined.

This is basically the same technique as we have applied at the current likelihood indicator but now is for the action plans. There still two options with the cloud and without the cloud. The source for the cloud stays the same because it is still internal and the access is also internally. But the level of difficulty is different because the Cloud provider are more protected. This will mean that the action plan does not have a strong effect. Without the cloud it is almost the same. The level of difficulty is harder for because they are not usually

so high quantified. That will take some extra fuss. In the orginal theory this was called Plocal$(p, t\alpha)$ but it is now called "Effect actionplan a" This leads to the following formulas:

Effect(Local) actionplan a = Source(0.20) * Access(0.15) * Difficulty(0.20)

Effect(Cloud) actionplan a = Source(0.25) * Access(0.15) * Difficulty(0.25)

Availability of a service
The same problem exists for this threat; there are some action plans that can be used to counter the threat. The solution to this vulnerability is to create more capacity. The source for the cloud is always external. Because the connection ot the cloud is external. The access is thus remote because the safety issues comes from outside. But the level of difficulty is structured and technical. Without the cloud this usually the same so the source is still external and the access is the same. Normal companies have less redundancy to counter the safety issue. So the countermeasure is still structured because it needs some planning but not technical. This leads to the following formulas:

Effect(Local) actionplan a = Source(0.20) * Access(0.15) * Difficulty(0.20)

Effect(Cloud) actionplan a = Source(0.60) * Access(0.20) * Difficulty(0.20)

6.5.1 Residual risk of threat

We have calculated the damage with the current indicator and now we are going to the same with the action plans. In the orginal theory this was called Rres$(p, t\alpha)$ but now it is called residual risk of threat t.

Data leakage:

Residual risk(Cloud) of threat t = Damage(0.40) * Likelihood(0.04)

To counter the data leakages a lot of action can be taken such as improve function separation and build in extra checks. So the impact and the type of loss can easily be reduced. The will we mean that the residual indicator will be much lower especially for the cloud provider because this is one of their hot topic and there will be a lot of funding for this problem.

Residual risk(Local) of threat t = Damage(0.40) * Likelihood(0.04)

The same approach will apply on the local part but there is one different this is not there core business. That is why the funding and the management priority will be lower. The type of loss will be different for them.

Availability of a service
Residual risk(Local) of threat t = Damage(0.40) * Likelihood(0.04)

It is difficult to do some against this safety issue. The most common option is to create more capacity. The will mean more funding for to address the problem. This is much easier for a cloud provider that a local company. Because the type of loss for the cloud provider will harm their business and that is different case for the local company.

6.5.2 Total residual risk of process

In this step the reduced risk for all the business processes will be calculated. The same formula is used as before only now is altered for the reduced risk. This is the total risk for all processes. In the orginal theory this was called $Rres(p, \pi)$ but now it is called "Total residual risk of process p".

Total residual risk of process p = $\sum_{p \in P}$ Rres(0.012)

The residual IS aggregated risk indicator also needs to be divide by 2 otherwise it can be above 1.

6.6 Classification

A classification must be determined based on the total risk. To do this the information of the risk indicators of the local and cloud values will be used. These are the basis for the classification. Because the values are different every time there are no static boundaries. For each threat differences into the local and the cloud value. That will indicated whether the risk is high. By multiply then the result with a 100 the risk is expressed into a percentage. Because the risk value is low it is just a moderate risk. Of course the management has to accept the risk. They can also adjust the investments in the action plans to counter the threats.

Total Risk = Total risk of process p(0.440) - Total residual risk of process p(0.012)
* 100

6.7 Business Rules

After the classification part the next part would be to use the business rules approach to determine which rules should be selected. But due to some circumstances this is not possible.

We could not finish the last and most important part. This part cloud not be used as a validation part.

7 Margin of error

In this section, the margin of error will be explained. The margin of error will be used in the risk analyis technique to improve the estimantion of the domain expert. The formula with a margin of error is showed below. The symbol δ entails the margin of error of each guardian as is stated in Section 4 Business Rules. The δ is number that is based on the opinion of a domain expert. The focus of the formula is not to determine a margin of error but it is about adding it to the numbers to improve the estimation of the domain expert. How the formula is build will be explained briefly.

$$\text{Local}(c) = 1 - (\pi_{i=1}^{n}(1 - \text{L}(Bi) + \delta_i)$$

Let us presume that are 3 guardian that need a margin of error. This will entail that n = 3. The symbols B1, B2 and B3 stand for the guardian and the symbols δ_1 , δ_2 and δ_3 stand for the margin of error. This entails the following the formula.

$$(1 - b1 - \delta_1)(1 - b2 - \delta_2)(1 - b3 - \delta_3)$$

Because the formula is a bit long the guardian will be reduced until the symbol A. This means that the part of 1-B in referred to as A1. The symbol δ stays the same.

$$(A1 - \delta_1)(A2 - \delta_2)(A3 - \delta_3)$$

The next step is to calculate the combinations together. This results into the following calculation.

$$A_1A_2\delta_3 - (A_1A_3\delta_3 + A_2A_3\delta_1) + (A_1\delta_2\delta_3 + \delta_1A_2\delta_3 + \delta_1\delta_2A_3) - \delta_1\delta_2\delta_3$$

But the formula can be reduced to the smaller form. That will be done in the following three formulas. Each step will reduced the symbols in the formula until it has the smallest form.

$$Error = -(A_1A_2\delta_3 + A_1A_3\delta_2 + A_2A_3\delta_1) + (A_1\delta_2\delta_3 + \delta_1A_1\delta_3 + \delta_1\delta_2A_3) - \delta_1\delta_2\delta_3$$

$$Error = -(A_1A_2\delta_3 + A_1A_2\delta_2 + A_2A_3\delta_1) + (A_1\delta_1\delta_3 + \delta_1A_2\delta_3 + \delta_1\delta_1\delta_3) - \delta_1\delta_2\delta_3$$

$$\frac{Error}{Value} = (\frac{\delta_3}{A_3} + \frac{\delta_2}{A_2} + \frac{\delta_1}{A_1} + (\frac{\delta_2}{A_2}\frac{\delta_3}{A_3} + \frac{\delta_2}{A_2}\frac{\delta_3}{A_3} + \frac{\delta_1}{A_1}\frac{\delta_2}{A_2}) - \frac{\delta_1}{A_1}\frac{\delta_2}{A_2}$$

This can be reduced until following formula. This implies that the formula is numeric stabile. By dividing the δ with the guardian it will incorporate a margin of error in the used numbers if necessary.

$$\frac{Error}{Value} = (\frac{\delta_1}{A_1} + \frac{\delta_2}{A_2} + \frac{\delta_3}{A_3})$$