Virtual Desktop and Cloud Services: New Security Demand

Blerta Lufaj

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2012

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Virtual Desktop and Cloud Services: New Security Demand

Blerta Lufaj

1st of July 2012

I dedicate this work to my fiancé Kamer and my dearest parents!

Abstract

Recently, the adoption of cloud services has led to several security concerns. Cloud services in most cases have benefits on reducing the cost and increasing the flexibility. Cloud adaption may cause several security concerns mostly but not the only ones regarding to data privacy, location and data classification. However, in cloud infrastructure technology approaches are mostly investigated by leading concerns into human aspects. The project is mainly focused on treating human aspects and their indication into cloud environment. Moreover, to elaborate the people's indication and make them positive factor in preventing and making the data in the cloud secure instead of being a disruption and factor of leading security incidents. To perform security measures and make cloud users aware of potential security risks, companies should provide policy statements and develop awareness programs.

Nevertheless, based on literature review and interviews done during this project with key persons in cloud security, we have treated main elements by focusing in the current and future approaches in order to deal with human aspects indication in cloud. Furthermore, the project examines the methods how to behave and how to make the cloud environment secure by building security measures, as well as how to handle if any incident has taken place within a company. Ultimately, the outcome of the project includes overall recommendations in how to make the cloud environment secure by treating main concerns and using appropriate security measures.

Acknowledgments

First of all I want to thank my supervisor, Prof. Dr. Bernhard M. Hämmerli for his support during the thesis project. He has been always available for discussion by giving useful advices, guidance and support. Mostly I appreciate his encouragement and his belief on my work by giving me motivation in the most difficult project stages and also for his help on finding the key persons to participate in the interview process.

I want also to thank and express my gratitude to the following individuals for being part of the interviews: Ole Tom Seierstad-Chief Security Adviser at Microsoft in Norway, Angelo Casanova-Senior IT Systems Engineer at ETAVIS GNS AG (Switzerland), Vidar Sandland and Peggy Sandbekken Heie-Norwegian center for Information Security NorSIS

I would like also to thank my fiancé Kamer Vishi for his support and gratitude during the entire period of studying. Finally, I would like to thank my family for keeping me more motivated and enthusiastic for this project.

Contents

List of Figures

List of Tables

1 Introduction

1.1 Topic Covered by the Project

In the last few years in information technology the most developing area was cloud computing indicating on changing the IT architectural solutions by using virtualization and offering data storage and application [15]. Accessing cloud services using virtualized desktop on Smartphone's, laptops, netbooks (tablets) is very common by many companies worldwide.

Barrie Sosinsky in his book "*Cloud Computing Bible*" [16] gives an explanation of what cloud computing is:

> "*Cloud computing refers to applications and services that run on a distributed network using virtualized resources and accessed by common Internet protocols and networking standards.*" *And it is "a collection of objects that are grouped together.*"

Advantages of using virtual desktop are: always the same desktop in all devices, low operational cost and easy data storage on the cloud servers. Therefore, beside of many benefits there is a big concern when it comes to adapt cloud services such as security and the way of managing it [15]. Challenge of using cloud services is dealing with some of the associated risks such as data disclosure, ID theft, data privacy and environmental risk. Beside of technology issues a weak link within a company when it comes to information security and security systems is a human factor.

To achieve a desirable security state within a company when cloud services are used it is needed to make an appropriate strategy and implement security measures including all factors indicating on security performance [17]. Therefore, adapting all security factors including technology, human factors and processes helps on improving security performance. According to NIST the most important but not the limited one of security requirements considering security needs of the company across a number of capacity includes: *privacy and confidentiality, integrity, data controls and access policies, governance* and *legal compliance* [18].

During the thesis project would work on treating the most common security concerns related mainly to human aspect and giving recommendation how to deal with these gaps indicated by factors mentioned above.

1.2 Keywords

Information Security, Cloud Computing, Cloud Services, Virtual Desktop, Human Aspects, Security Policies, Access Control, Data Center, Cloud Security Awareness.

1.3 Justification, Motivation and Benefits

Cloud services have lately raised attention worldwide, adapting its services by many companies caused a new challenges. However, cloud providers have launched many services and products a big concern when companies moving from traditional IT infrastructure to the virtualization infrastructure is cloud security [19].

Therefore, the organization management should prioritize security risks and implement controls protecting systems and information. ENISA recommends all companies before adapting any of cloud services first to develop a risk assessment, make an appropriate decision to collaborate with cloud providers based on company needs, and choose certain cloud services in order to make easier the security maintenance.

Technology system protection, human aspects and controls have critical indication on performing good security, but even if all these strategies are performed it does not mean that any security incident may not happen at any time. Goal of this project is to describe security concerns and to help on improving security performance within an organization.

1.4 Choice of Methods

This section describes the method used during this thesis project. The intention was to choose the appropriate method in order to describe and treat the problem in a proper way. In cloud infrastructure the data are usually shared with cloud vendors, and there are many technical and management methods that are used but human side and the impact of people is much less investigated.

The method used was based qualitative research methods and on semi structured interviews. "*Qualitative research aim to gather in-depth understanding of human behavior and the reasons that govern such behavior*" [20].

In the interviews session has participated security experts with many years of experience. They had different backgrounds but one of them was expert in cloud computing. This interview method was chosen because of the possibility to have better collaboration, using second options in case of giving improper answer to have the chance to make follow-up or sub questions.

1.5 Research Questions

In this project the following questions will be described:

1. Market and Competition analysis:What are the current platforms that provides virtual desktop and cloud services: advantages and disadvantages?
2. How to identify the current security gaps related to technology, processes and human aspects?
3. How to design solutions to deal with the identified security gaps related to technology, processes, monitoring (traces) and human aspects.
4. What are presumptions to business, that it accepts secure solutions?
5. What are the methods of preventing security incidents caused by technology, processes and human aspects on Cloud Services?

1.6 Planned Contribution

Goal of this project is to find out solutions on protecting cloud services and virtual desktop focusing not only on technology systems as many researches are done but trying to elaborate also with processes and human aspects and try to optimize this triangle in one outcome solution.The project will cover some of security measures in the cloud where enterprises should make step-

changes in the level of awareness, care and classification of the information and security among its staff. However, even the company is having support and control performance over the virtualization infrastructure by the cloud provider, still the company need to recognize that this may be not enough without treating the role of the user in classifying and protecting information.

1.7 Thesis Outline

The thesis is structured as follows and an outline diagram is given in figure 1:

Chapter 1: introduces the research problem, research questions and methodology.

Chapter 2: describes the state of the art in cloud computing and security issues.

Chapter 3: highlights the security management in cloud and processes used to manage possible vulnerabilities involving management procedures to build an appropriate transparency for cloud services, in order to manage properly the governance and to implement preventive and detective security controls to make more secure the data in the cloud.

Chapter 4: presents the incident handling and the way of managing it by exploring costumer's and vendor's responsibilities.

Chapter 5: describes mostly the main virtualization providers, their offered services and strategies provided by them.

Chapter 6: presents three main security indicators: technology, processes and human aspects by treating each of them in more details, and as well as some of security issues when virtual desktop and cloud services are used.

Chapter 7: describes the interviews results and security experts claims giving their presumption in different cases regarding to the content of the topic.

Chapter 8: in this chapter is presented a short discussion extracted from interviews analysis.

Chapter 9: concludes the studies with main results and future work.

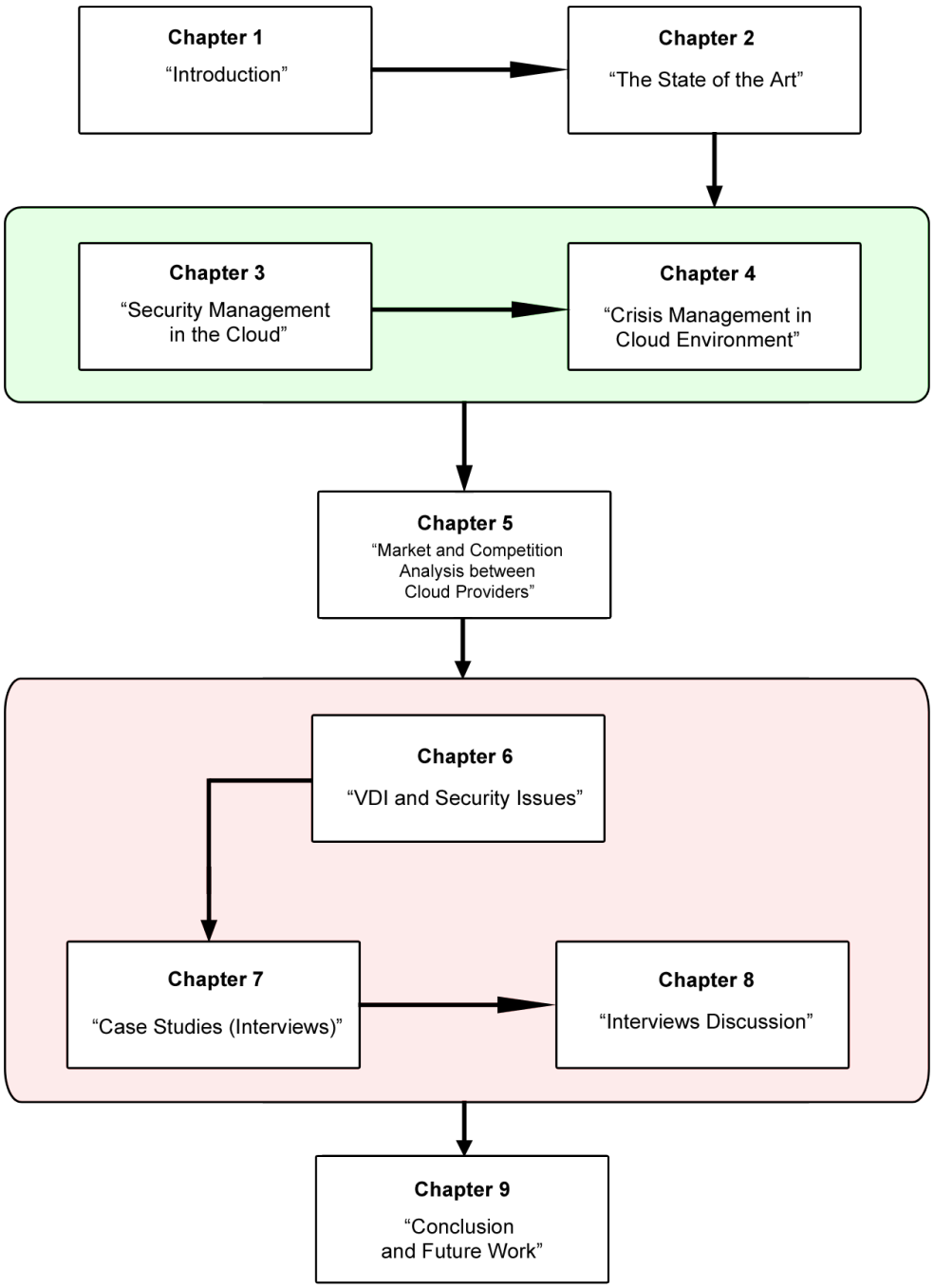

Figure 1: Master's Thesis Outline.

2 The State of the Art

National Institute of Standards and Technology (NIST) has defined cloud computing [1] as:

> "*A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*"

Cloud computing provide fast and cheap computational offering to the market data storage and capacity. Security importance and concerns starts when application runs beyond firewall moving closer to the public domain. Cloud computing make possible to use its services based on demand, as a self managed service in virtualization infrastructure. Cloud services are built by sophisticated automation, management and virtualization technology, having huge difference from previous IT models; it moves software and data from the physical model to virtualization infrastructure. Cloud computing transforms IT model from cost center to the service provider model [21].

There are many cloud computing definitions such as Oracle's CEO L. Ellison [22, 23] claims that:

> "*cloud computing is nothing more than everything that we currently do*".

Also five essential characteristics for cloud services are identified by NIST [18, 1]:

1. On-demand service,
2. Broad network access,
3. Resource pooling,
4. Rapid elasticity, and
5. Measured service.

Cloud computing infrastructure and its services are launched by many companies worldwide. Characteristic of cloud computing is the computing processed via the Internet as service [19]. Hence, computing and IT resources are consumed and delivered as a service without having a need to know details of how it is implemented, deployed, administrated and maintained. This makes possible transferring the systems from on-promise to the remote systems connecting users to the IT infrastructure via Internet. Establishing this transformation by individual companies indicates on losing their control over their IT systems because as said above the IT infrastructure will be provided over the Internet and it is leased from the cloud providers. Moving toward cloud infrastructure storing all data into cloud may cause security concerns [24] such as:

- Limited control over the data, causing security incidents

- Having the whole data provided by a single cloud provider may happen that the cloud provider controls and modifies tenant's data.

NIST has defined several deployment models, and provided distinct models implementing based on company needs when migrating applications to a cloud environment.

Deployment model defined by NIST [18, 1] are as follows:

Private Cloud- operates exclusively only for an organization, and cloud may be managed by that company or by a third party. Private clouds may be on or off premise.

Public cloud - means that cloud infrastructure is available to the public or to the large industry group owned by a company which sells cloud services.

Community cloud - means that cloud infrastructure is shared for more organization, and these organizations have same concerns with each other such as their purpose, security, policies and compliance regulations. This kind of cloud infrastructure may be managed by a third party or by the organization.

Hybrid cloud - is a combination of two or more cloud infrastructures such as private, public or community. In this case clouds have their particular identities but are linked together as a unit.

In the figure 2 is shown the visual model of working definition for Cloud Computing by NIST.

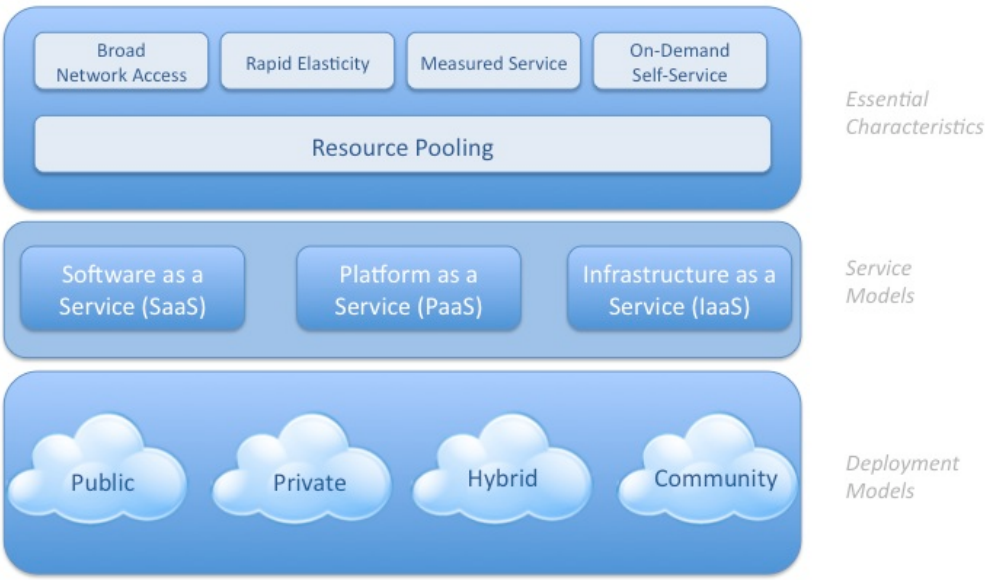

Figure 2: The deployment and service models of Cloud Computing [1].

There are different types of cloud when it comes to the deployment model. A sample description is that client's network, management, and responsibilities starts and ends with cloud service provider's responsibilities.

Based on organization needs different vendors offer different services called service models. All service models have its common purpose XaaS or Something as a Service. Three main types of cloud services are:

Infrastructure as a Service (IaaS)- the purpose of IaaS is to provide virtual machine, storage, virtual infrastructure, and other hardware resources which are very useful for clients. The entire managing infrastructure is responsibility of IaaS service provider, but clients should take care and control for other issues such as operating systems, applications and also the correlation between users and systems. In the figure 3 are presented service models in the cloud and their way of managing along with comparison between them and traditional IT infrastructure [5, 25].

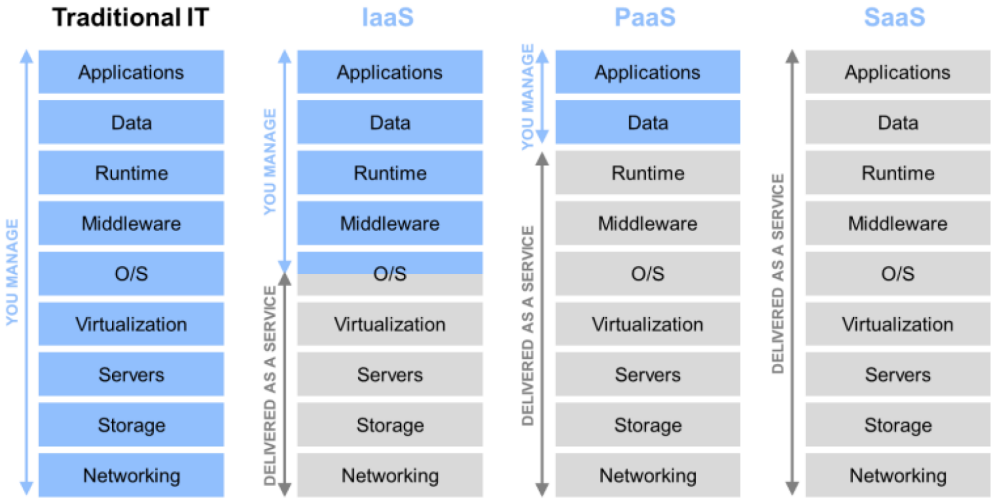

Figure 3: Cloud computing service models [2].

Platform as a Service (PaaS)- makes possible providing operating systems, applications, services and controlling structures. In this case clients are able to choose applications based on their needs which are on the cloud infrastructure or in other hand they can choose any of applications developed by using programming language and any of other assets that are provided by PaaS service provider. So, managing cloud infrastructure, operating systems, and software resources is service provider's responsibility [5, 25]. However, clients have other responsibility such as installing, developing and managing the application.

Software as a Service (SaaS)- provides completely operating infrastructure including management, application and user interface. In this model application runs to the client through a thin client interface. User's responsibility is to manage his own data, while vendor's responsibilities starts form the application and ends to the infrastructure. Software as a service (SaaS) is considered as the main model of cloud services and it is the main critical field when security should be implemented with good performance [5, 25].

Therefore, before adapting cloud services from any cloud vendor is needed to make research and analyze the provider's security policies of the data in order to avoid incidents causing data loss or incapability to access those data. There are seven security issues that should analyze with cloud providers before adapting its services defined by technology analyst and consulting company Gartner [26, 27]:

Privileged user access: the client should know who is managing its own data and have more information for the people with privilege administration and access control over the data.

Regulatory compliance: be sure that the cloud provider is always ready to take external audits and security.

Data location: it is very important for the client to know the location of the stored data while it could happen that the tenant is not informed about the country where the data are stored in. Cloud providers should explain about the process data storing, jurisdictions and local privacy.

Data segregation: perform encryption at all levels and make sure that encryption scheme was constructed and tested by professionals.

Recovery: cloud vendors should explain to the tenants about what may happen if any disaster occurs. Hence, when adapting cloud services from cloud providers, it is very important to get information about if the data may be restored after any possible disaster and how long it takes.

Investigative support: in cloud computing it is very difficult to investigate illegal activities. Cloud services investigation is almost impossible, while logging can take place in multiple locations with the possibilities of spreading across hosts and data canters.

Long-term viability: it is cloud providers responsibility to obtain the data and be available even after long time. Depends of the client needs the data should be ready to be imported from the current format into a replacement application.

2.1 Cloud Services established by cloud computing

According to the International Data Corporation (IDC) as a provider of market intelligence, has defined cloud computing as follows:

> "*An emerging IT development, deployment and delivery model, enabling real-time delivery of products, services and solutions over the Internet (i.e., enabling cloud services)*" [11].

And Cloud services are defined as:

> "*Consumer and Business products, services and solutions that are delivered and consumed in real-time over the Internet*" [11].

When cloud computing is mentioned, people think about the online delivery services and the use of different models contributing on business and consumer services. However, these services are referring to the IT services like SaaS and storage of the data as a service but also many more non IT business and services.

Hence, cloud services are enabled by cloud computing environment consumed and delivered over the Internet.In the figure 4 are presented the service delivery models and cloud computing deployments [3].

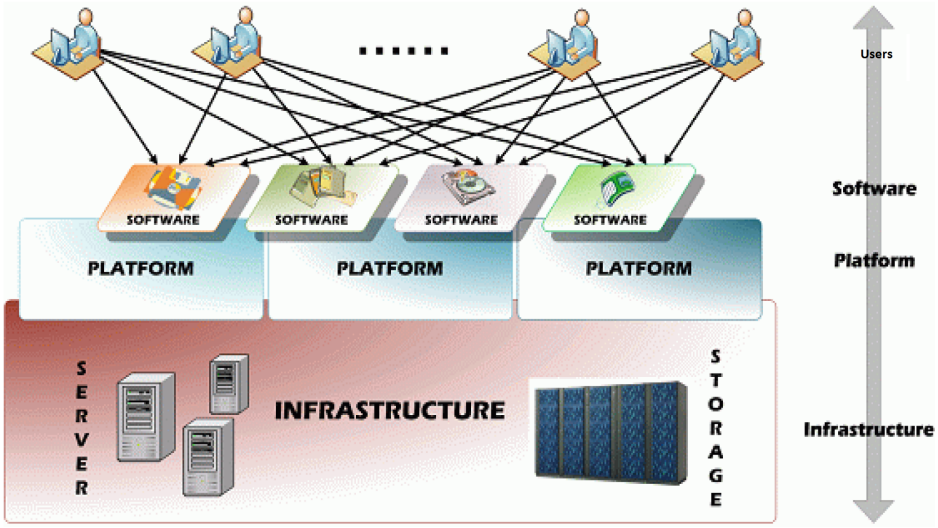

Figure 4: Cloud computing layers [3].

2.2 Virtual Desktop Infrastructure

Most of the organization wants to adapt technology infrastructures that makes possible fast delivery services to the market. Hence, Virtual Desktop Infrastructure helps on dealing with these challenges by improving the IT agility, business outcomes, reduce the cost and improvement of business recovery strategies [4]. Usage of cloud computing is increasing rapidly, moving virtualization to the next step. The next level for organization infrastructure is desktop virtualization known as Virtual Desktop Infrastructure (VDI) [12].

Virtual Desktop Infrastructure is completely different from desktop virtualization offered by CPU vendors, using methods of virtualization of multiple operating system or application running on a single device. However, VDI establishes virtual desktop machines running on servers within the data center [28]. Virtual Desktop means that standard desktops converted as virtual machines making possible to access by the users through different devices, such as desktops, laptops, mobile devices, Smartphone's and tablets. In figure 5 is depicted the connectivity of different devices from different places into the virtual desktop.

VDI improves the system management and makes possible to manage the virtual machines centralized in data center and in return to give a full PC desktop experience to the user. Moreover,

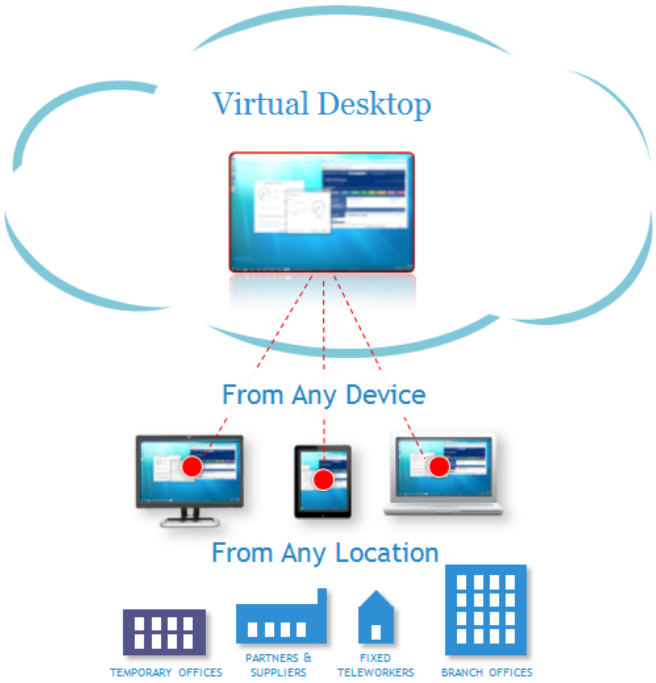

Figure 5: Virtual desktop access

VDI deployment administrators have ability to control all features and aspects of configured methods of the virtual machines. Virtual desktop has transformed the traditional "edge" into the data center [4, 12]. According to the [vDaaS] is used a new definition vDaaS with the meaning of Virtual Desktop as-a-Service which is compatible with DaaS definition.

Virtual Desktop as a Service (vDaaS) transforms the approach of delivering to the end-user virtual desktops seamlessly through a cloud services enabled by the data center. Moreover, DaaS is defined by [29] as: "*Combination of cloud services and virtualized desktops*".

The Solution provides an easy manageability and also an easy adoption of technology modifications in desktop infrastructure by delivering cloud services to the personalized desktops running anytime and from anywhere. Moreover, virtual desktop has ability to provide access via a thin-client or any other device. VDI support the manageability of the enterprise-class, controlling without compromising end-users experience [4]. Figure 6 presents the architecture of all layers in VDI including storage, network, process of computing and virtualization.

Virtual desktop is considered as important strategy because of the impact on reducing the cost and complexity of managing an expanding of different devices. Hence, by establishing organization to the centralized desktop deployment and management, VDI by improving and investing on security, establishing impact on increasing business agility and IT flexibility, improving business continuity and disaster recovery. Moving to virtual desktop infrastructure means that all components: storage, processor, memory and networking are moved to a centralized data center [30].

DaaS provides several benefits described in [29] , are listed as following:

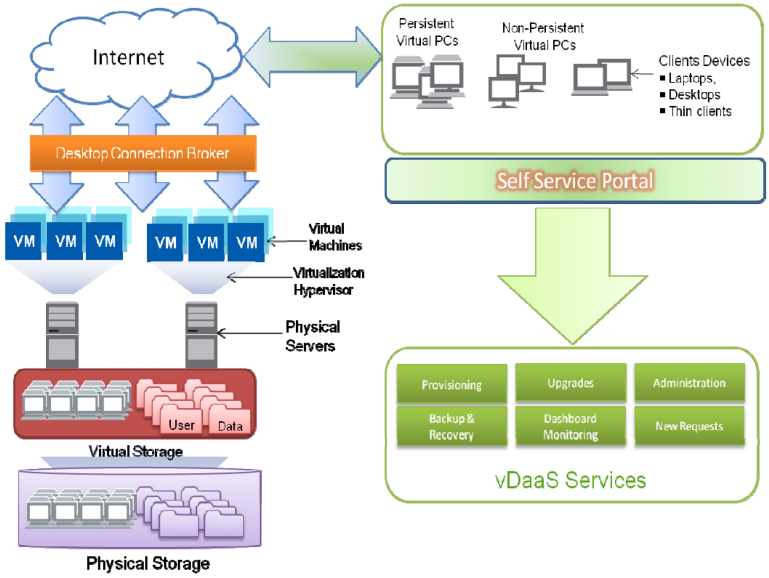

Figure 6: DaaS Architecture [4].

- Management of PCs
- Improvement on security
- Disaster recovery and business continuity strategies
- Indication on reducing the cost
- Indication on reducing hardware expenses
- Fast deployments
- Provided better support and reliability
- Possibility of accessing into the newest technologies

However, there are also many disadvantages regarding to DaaS as presented below:

- The high amount of required Bandwidth
- Concerns regarding to license
- Issues related to Data ownership
- Compliance worries and issues
- Customized applications
- Requirements of vertical market software and hardware
- Concerns related to security

3 Security Management in the Cloud

Adapting cloud services using public cloud deployment model means that many information and a part of network, application, system and data of the company are controlled by vendors as a third-party. Cloud services are able to create clouds (islands) of virtual perimeters sharing the responsibility as a security model between costumer and the cloud service vendors. Shared responsibility may indicate on causing a big challenges regarding to the security management for the IT staff and for the whole organization [31].

The most important point for the company and its management is to have the ability to answer the question if the company is having the appropriate transparency from cloud services in order to manage properly the governance and to implement preventive and detective security controls making sure that the data of the company stored in the cloud are well protected. There are two important things when it comes to answer this question such as: determine the customer needs in order to implement security controls in the cloud platform, and what the company should involve to adapt security management tools and processes needed for managing the security in the cloud. Both of the security indicators should continually reevaluate depending on the data sensitivity and the changes on the service-level over time [32].

Costumers should make exercises to understand the trust boundary for services used in the cloud. It is obviously needed to understand all the layers within the companies touch or interface in the cloud such as network services, host level, application level, database, storage, and web services including identity services presented in the figure 7. Thus, to fulfill the company needs it is necessary to know the scope of the IT system management and monitoring responsibilities that the company is in charge to involve including access, configuration, change, patch, and vulnerability management [5].

Even though there is a possibility to transfer some particular responsibilities to the cloud provider but still it depends on different factors, including the service delivery model used, service level agreement signed with the provider, and the capabilities obtained by the provider to support continuously the company regarding to the internal security management processes and tools.

Large companies are usually interested to adapt security management frameworks like Information Technology Infrastructure Library (ITIL) and ISO/IEC 27000 service management framework. Hence, these frameworks provide companies with guidance about planning and implementing a governance program keeping up management processes indicating directly on protecting information resources [33].

For example, the service management framework Information ITIL (Technology Infrastructure Library) depicts a detailed explanation for the most important IT practices comprehensive checklists, tasks, and procedures that can be adapted by many companies. A key principle of ITIL when cloud computing is applicable in the company is that people, processes and information systems are changing every day.

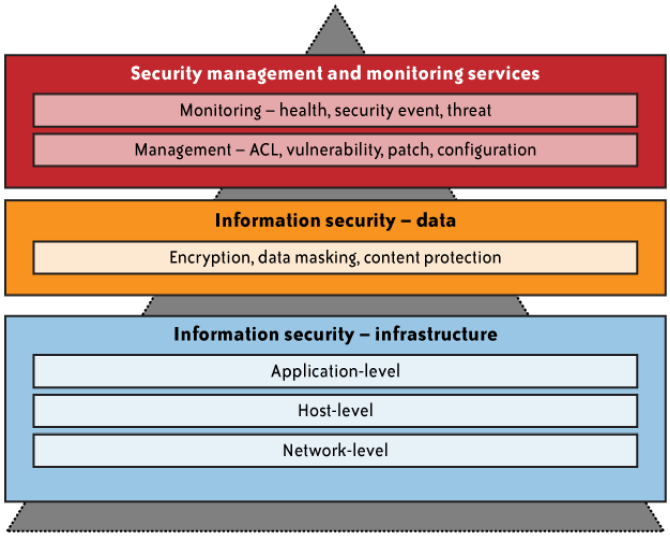

Figure 7: Security management and the process of monitoring [5].

Therefore, ITIL as one of the management frameworks will continuously improve the necessary requirements to align and realign IT services based on organization needs. Continuous improvement means the focus on identifying and improving IT services in order to support business processes. Having in mind the dynamic of cloud services, the activities presented within the security management processes should involve the process to be continually revised to remain current and effective. Hence, security management is considered as a constant process which is similar and relevant to cloud security management [5].

The main goals of the ITIL security management framework are:

***Realization of security requirements*:** Service-level agreement (SLA) usually define security requirements including also external requirements related with contract support, legislation and internally or externally policies.

***Realization of a basic level of security*:** This makes possible to perform an appropriate security within the organization and guarantee the business continuity reaching the service-level management for information security management. Security management processes established in the right way are close connected with IT policies and standards of the company, having the main goals to protect the confidentiality, integrity, and availability of the data.

In the figure 8 is illustrated the ITIL life cycle in an organization. Disciplines of the security management are represented by relevant ISO and ITIL functions.

According to the book *Cloud Security and Privacy* [cite here] based on ITIL and ISO frameworks analysis were identified the most recommended security management for securing cloud services:

- *Availability management (ITIL)*

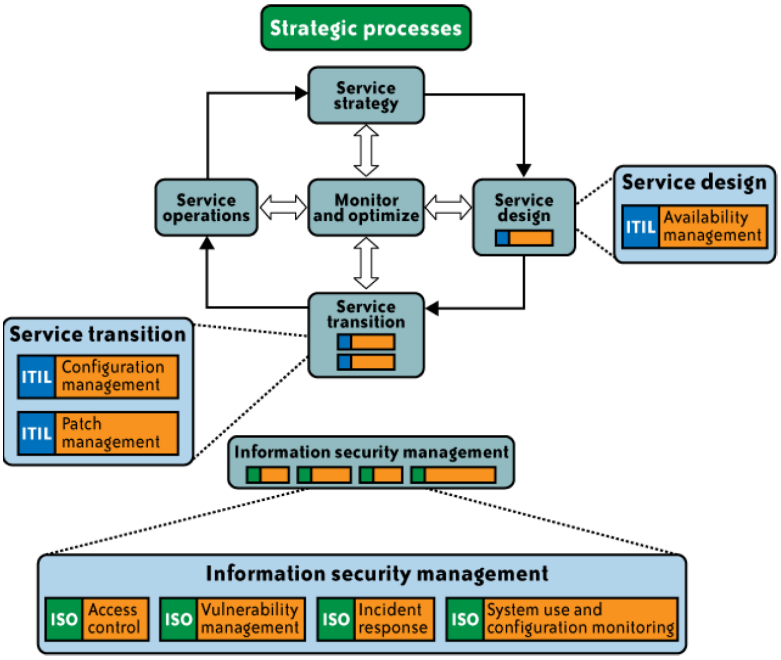

Figure 8: ITL life cycle within the enterprise [5].

- *Access control (ISO/IEC 27002, ITIL)*
- *Vulnerability management (ISO/IEC 27002)*
- *Patch management (ITIL)*
- *Configuration management (ITIL)*
- *Incident response (ISO/IEC 27002)*
- *System use and access monitoring (ISO/IEC 27002)*

Security management processes were chosen based on the impact that they have on performing security and the risk they cause without well treating. There is different security offered by different cloud deployments and delivery models. However, this area is evolving every day, and it is very important to reexamine capabilities of the cloud services and analyze appropriately the security management processes. In the table 1 are depicted different security management processes accessible for each of the SPI cloud delivery models in the context of deployment models. It is well shown that security management practice depends on the type of the delivery and deployment models.

3.1 Security Concerns in Cloud Management

The major threat when using cloud services is the possibility of exploiting vulnerabilities of infrastructure, network services and applications. The risk is even higher for the public PaaS and IaaS delivery model where the costumer is responsible for managing the vulnerability, patch and con-

Table 1: Management functions for SPI cloud delivery models

Cloud deployment/SPI	**Public clouds**	**Private clouds**
Software-as-a-service (SaaS)	• Access control (partial) • Monitoring system use and access (partial) • Incident response	The following functions typically managed by your IT department or managed services: • Availability management • Access control • Vulnerability management • Patch management • Configuration management • Incident response • Monitoring system use and access
Platform-as-a-service (PaaS)	The following are limited to customer applications deployed in PaaS (CSP is responsible for the PaaS platform): • Availability management • Access control • Vulnerability management • Patch management • Configuration management • Incident response • Monitoring system use and access	
Infrastructure-as-a-service (IaaS)	• Availability management (virtual instances) • Access control (user and limited network) • Vulnerability management (operating system and applications) • Patch management (operating system and applications) • Configuration management (operating system and applications) • Incident response • Monitoring system use and access (operating system and applications)	

figuration. Costumers should understand the importance and the responsibility that they have on performing the security and managing it in an appropriate manner. To get well informed about the cloud security and the security management functions, costumers should demand support from cloud service provider (CSP) [34].

To deal with vulnerability, patch, and configuration usually the main responsible part are cloud service providers which are responsible to manage the infrastructure. The most sensitive

area for companies is considered data security and privacy and as a security issue is considered the possibility of unauthorized access.

3.1.1 Security issues in Cloud

Performed security measures would indicate on keeping sensitive business information safe and out of reach from unauthorized people, while we are describing and analyzing services offered by public cloud where the users have ability to access the data via Internet anywhere and anytime.

According to the paper "*Cloud computing security issues and challenges*" [35] the authors has described some of the security issues, which are summarized below:

Security concern 1: Using cloud infrastructure has less indication on performing good security because of sharing its own resources with any other company, without being informed where the data are stored on.

Security concern 2: It may happen that company has not fulfilled regulation according to the law and the data may be seizure by the government

Security concern 3: Always there is a possibility of occurring a problem when the data stored into one cloud provider moving to another cloud provider

Security concern 4: There is an important issue when it comes to the information of who controls and monitors the encryption and decryption keys. It should be managed and controlled by the costumer.

Security concern 5: Protect the data of being modified from any unauthorized person. In order to protect the integrity of the data still there is no developed standard.

Security concern 6: When Payment Card Industry Data Security Standard (PCI DSS) is used the data logs should perform in according with security managers and standards.

Security concern 7: The application performed by the users should be kept up to date to ensure that they are good protected.

Security concern 8: When it comes to store the data about particular citizens there are many states having strict regulation by the government on what data can be stored, defining also the duration of the data can be stored, thus some of the banking regulators decides if the customer's financial information should stay at their home country or not.

***Security concern 9*:** The virtual machines are categorized with very dynamic nature making difficult to perform with good security.

Security concern 10: In case of being violated with the data privacy by the cloud vendor always exist the possibility for the costumers to sue cloud vendors, indicating on losing the reputation of the company and as a result causing a huge damage.

3.1.2 Management of Security Vulnerabilities

Vulnerability management helps on protecting hosts, network devices, and applications from being attacked through known vulnerabilities. Many companies developed a vulnerability strategies in order to make possible systems scanning which are connected to the company's network, assess the risk causing vulnerabilities to the company, and the remediation process to face with these risks. Hence, to be protected against these vulnerabilities a good practice is to implement technical vulnerability management in an effective systematic and repeatable manner with taking prove of its effectiveness [5, 36] .

3.1.3 Patch Management and Security

Comparing with vulnerability management, security patch management is quite similar, given that protects hosts, network devices, and application as a vital threat management, and helps on preventing exploiting vulnerabilities from unauthorized users. Security patch management makes possible to sort the threats categorizing them as insider or outsider threats [5].

3.1.4 Security Performance in Management Configuration

It is used to protect hosts and networks devices from exploiting configuration weaknesses, and is similar to the vulnerability management program and it is considered as a subset of overall IT configuration management. Security configuration management provides security on monitoring and access control when used critical systems and database configuration files, including: firewall policies, network zone configuration and management of access control [5].

3.2 Concerns in Identity and Access Management (IAM) in Cloud Environments

Identity and Access Management (IAM) is defined as one of the protection factors of the company regarding to the information security, through particular rules and policies adapted by the users via various methods such as request for login passwords, defined privileges and provisioning user accounts. Nevertheless, to provide protection for the organization resources, privacy and protection of users personal information do not exist any restricted rule. However, most of the companies provide their security through adequate user's identity management and privacy [5].

Challenge of IAM is considered the concern of managing access for users while accessing internal and external services. Challenge of IT is the rapid changes into users or employees profile where their role and responsibility is changed often for business reasons. Organization works on providing and performing better security, regulatory compliance and reputation risks. Facing with these challenges, companies mostly has developed technology solutions to provide centralized and enable automated access management for the users. Organizations should provide strategy and architecture for their IAM because of achieving success on their business functions [5, 36].

4 Crisis Management in Cloud Environment

4.1 Incident Management Process

Incident response signifies on that the organization should develop methods to deal with possible attacks and with their consequences [37]. In cloud infrastructure where the company is using public cloud and the cloud is provided by Cloud Service Providers (CSP) as a third party, the role of providers is as well as important on performing incident response activities, including verification of the incident, attack analysis, containment, data collection and preservation, problem remediation, and service restoration. Cloud providers may monitor and control each layer of the cloud application: including application, operating systems, network, and database. Below are described the incident management processes [6]:

- **Incident detection and recording:** Through monitoring systems and also with the help of the users, the incident would be handled by the IT group in different stages.
- **Classification and initial support:** All the incidents should be categorized and classified through three main criteria: Priority, impact, and Urgency. Hence, one of the most important areas when an incident has taken place is to define the priority of the incidents. Therefore, the Service Desk is responsible to define priorities using appropriate, standardized coding criteria and then the next level is to resolve the incident.
- **Investigation and diagnosis:** During this phase, operators are focused on trying to find and identify the cause of the incident according to the historical incidents and known errors, and it is important that the operators keep saving the action taken to resolve the problem by updating the incident record.
- **Resolution and recovery:** The solution of the incident or workarounds obtained from previous steps taken to resolve the incident will be applied on the current incident situation.
- **Incident closure:** Another responsibility of the Service Desk is to check the current status of the incident and based on the state close the process.
- **Incident monitoring and tracking:** During the incident phase the governors need to have information about the incident state and prevent incident escalation in time.

Nevertheless, tradition processes applied are not applicable for the cloud computing environments, while it is a pool of virtualized computing recourses. Cloud computing provide fast computational recourses offering to the market data storage and capacity. Characteristics of cloud computing are:

- **Large-scale:** Cloud data center is build by many ordinary servers and other devices.
- **Virtualization:** Making possible for the user to access cloud services via the Internet without having the need to know how the service is running in the cloud.

In figure 9 is shown an improved incident management process in cloud computing environments, based on [6].

According to [6] the improved incident management process in cloud computing is defined as follows: "*Compared with the traditional incident management process, the new process introduces a mechanism of incident predication and a process of incident prioritization. Both improve the efficiency of the incident management process*".

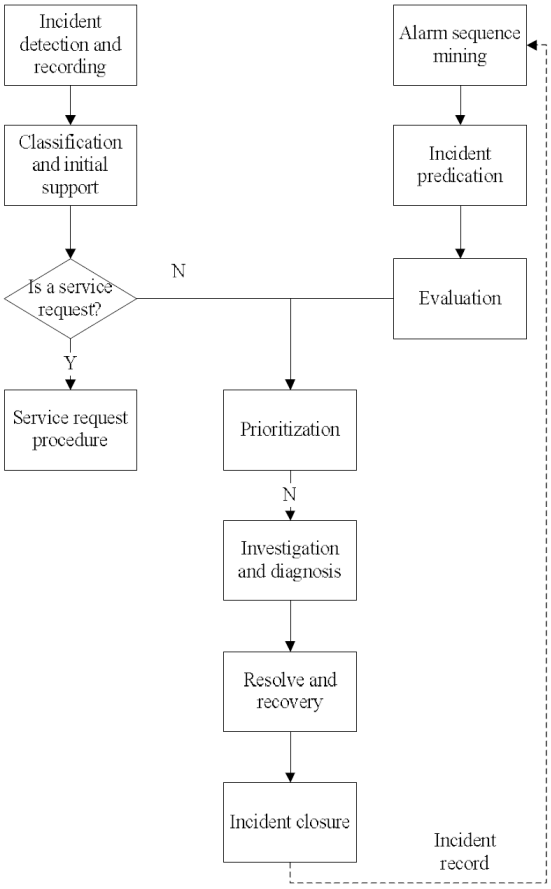

Figure 9: Incident management process for cloud environments [6].

4.2 Cloud Management and improvements in security incidents

Most of the medium and large companies perform security and incident monitoring process using internal security operations center or a third party services. The Security operations center makes possible monitoring of each event from firewall and intrusion detection systems (IDS), and depending on the situation react and respond by using Computer Security Incident team (CSIRT). Hence, using cloud services is the current trend by most of the companies worldwide meaning that cloud application deployment brought many challenges regarding to the security monitoring model as long as cloud application will not be protected only by monitored firewall

and IDS.

In the cloud the monitoring and incident response depends on the SPI (Service Provider Infrastructure) delivery model, incident disclosure policy, SLA (Service-Level Agreement), and data governance model provided by Cloud Service Provider (CSP). In order to handle and respond appropriately for any security event reported,is necessary to define responsibilities and procedures in order to react in incident cases. Incident response in cloud is not the same as used for IT traditional models where the incident response process was notified and handled by internal groups within the company responsible for all its IT applications. Incident response in cloud depends on the nature of incident where the cloud providers may be involved as well.

Using thousands of application on the cloud makes much more complex the situation of managing incidents. Hence, to respond in an effective way it may help a tool provided by CSP to manage the complexity of application [5].

4.2.1 Incident Response Plan

If any incident takes place and it is verified that is not a false alert it means that is only the beginning and the company should have developed a plan including a number of different levels based on the incident severity. The incident will be categorized in various ways such as low, medium, high, major and minor, based on this classification would come an appropriate response for each of them.

As in IT traditional infrastructures, in cloud environment as well is needed the management of systems for monitoring and providing notification of security vulnerabilities continuously through automated technology systems. However, to protect the organization from any potential incident is not just enough providing advanced technology systems. Given that, one of the main factors indicating on preventing incidents are users inside the company, so concerning it, the best method is developing policies and regulations. Hence, without this capability and expertise in information security, a company would not successfully face with detecting and preventing security vulnerabilities of its costumer's data and providing service availability.

4.2.2 Computer Security Incident Response Team (CSIRT)

The company should arrange people who have responsibility to analyze, monitor, and react if there is an attack taking place. Still it is almost unclear if the CSIRT may provide the same security in cloud environment as in the IT traditional infrastructures. However, the indications of causing an incidents in cloud can be much more severe. Benefits of using cloud services are already known, however the main concern is security and another important thing it is how to make an appropriate incident plan without impacting business continuity and how to accomplish with the legal aspects which are not clear enough until now [7]. To handle any kind of incident within a company, CSIRT is having main tasks [7, 38]:

- Incident report
- To analyze the event notification
- Response to an identified incident
- Provisional Authentication Decision,

- Post-incident follow-up, and
- Reporting to the appropriate parties

Figure 10 presents the activities of handling security incidents using cloud services.

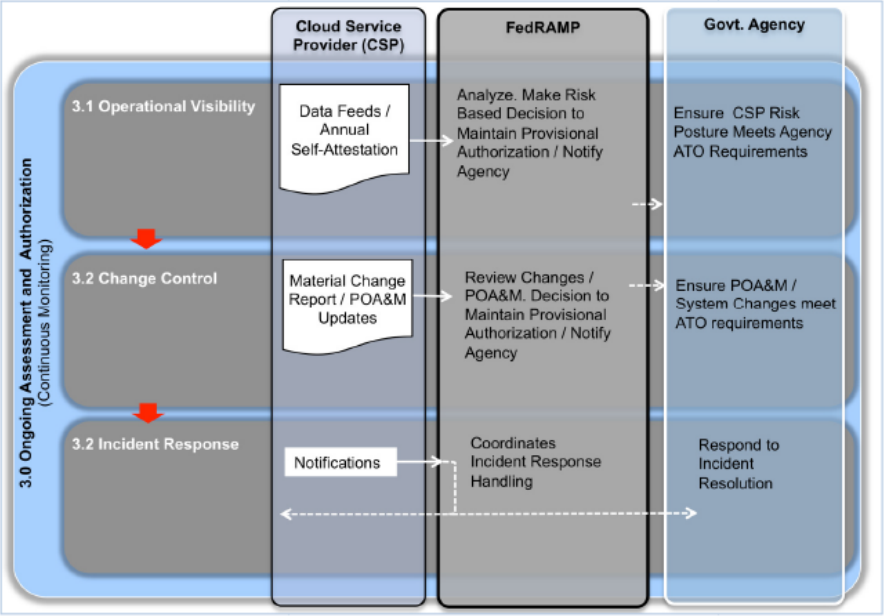

Figure 10: Incident response activities using cloud services [7].

4.3 Disaster Recovery Requirements

In cloud environment the capability of disaster recovery strategies and their capacity of on-demand resources may be used for performing better resilience when faced with increased service demand or DoS attacks, and quickly recover from being faced with serious incidents [37].

In this section are described briefly key requirements for performing an effective disaster recovery process, therefore some of the requirements depends on business decisions.

- **Recovery Point Objective** for the disaster recovery systems represents the key points where most of the data are stored, where facing with potential attacks would have high impact.
- **Recovery Time Objective** determines the time needed for being recovered after a failure occurred.

Performing successfully the Disaster Recovery services in cloud infrastructures means that the impact of any failure occurred is minimal and the performance of the business operations are continuing without disruption [8].

4.4 How Disaster Recovery works today?

The performance of disaster recovery services in cloud environment would work better by replacing all the data and cloud application in more than one data center, helping in any possible incident situation, where data stored in the main data center becomes unavailable to have the option of accessing the backup data into another data center being able to perform the service availability and business continuity [39].

Backup policies and procedures performed by the organization have great indication on improving the security within a company; however cloud providers performing the same procedures as the company may be even more robust on preventing security incidents [40].

Having the data in cloud makes possible of being available, faster to restore and more reliable in many sides comparing with traditional infrastructures, as well as having the ability of performing the backup process by storing the data in different geographic places. Nevertheless, service performance over the Internet and the capacity of data are considered as important factors on affecting restoration [5]. Critical implication may cause the unavailability and inaccessibility in the SaaS environment even for few moments. Given that, an important issue is the availability of software application.

Benefits of using virtualization regarding to business continuity and disaster recovery is the ability of delivering on service-level agreements and provide high quality service [5].

4.5 Disaster Recovery of Cloud Storage

Cloud makes possible the continuity of applications and the security of data through system structure for disaster recovery: "*distributed computing, centralized storage*". According to [8] there are three disaster recovery levels:

- **Data-level disaster recovery:** ensuring the security of data applications.
- **System level disaster recovery:** for operating system of application server, ensures that the time of disaster recovery to be as short as possible.
- **Application-level disaster recovery:** ensures the security of applications.

A typical architecture of disaster recovery systems is given in figure 11

According to the SNIA (Storage Networking Industry Association) [41], the data should be stored at least in **three different geographical locations.** Storage services in a shared public cloud can be placed in many private clouds, and it can be called "inter-private cloud storage". It does not offer services only for enterprise in private cloud with specialized storage services of disaster redundant backups, but also for the cloud users with convenient and efficient mobile service.

4.5.1 Factors causing security incidents

Disaster recovery methods have such rely on "declaring a disaster" in order to influence on the backup infrastructure during an occurring incident: hurricanes, tsunamis, floods or fires. Therefore, interruptions in availability of services occurs more as a result of everyday activities. However, organization should treat, develop response strategies and build disaster recovery plan, having always in mind the worst cases, but in the plan should be treated the most random cases

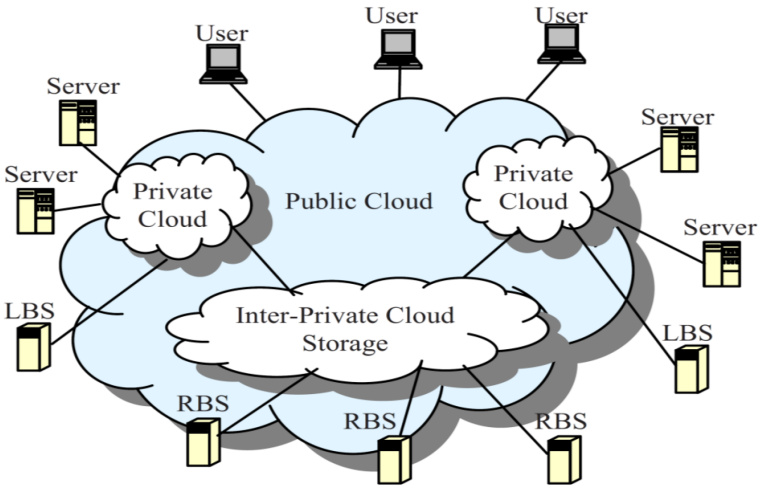

Figure 11: A typical architecture of disaster recovery system. Where RBS (Remote Backup Server) and LBS (Local Backup Server) [8].

such as cut power lines, server hardware failures and security breaches. More than 50 percent of the disasters occurred as a result of various factors [9]. This information refers to the statistics of the IBM clients which have declared a disaster. Hence, organization should plan the recovery of critical business operations instead of infrequent, momentous disaster and develop the plans accordingly. The figure 12 gives an overview of some types of disruptions in the past few years based on IBM statistics

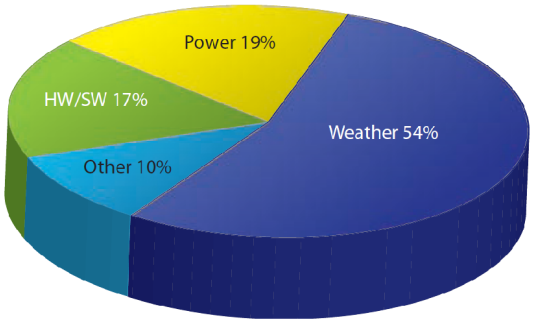

Figure 12: Indications of causing business interruptions [9].

4.5.2 Management and Factors of Cloud Services Availability

Cloud services have been facing with various incidents causing often outages and the impact caused by it was depending on the outage situation, the criticality of the cloud services and the relationship that they have with the business functions. If the incident affects any critical business application where the company must provide the continuous availability of service, even having outage for few moments may cause a serious damage to the companies productivity, customer

satisfaction, revenue, and service-level compliance.

On April 21, 2011 an incident with Amazon Web Services (AWS) caused service outage where many companies using its services were completely offline, nevertheless a company called Netflix survived from this disruption by performing normally its services. It has survived because of using some degradation in service, designing redundancy into its Cloud based infrastructure. The AWS outage did not reflect on Netflex because it has spread the cloud infrastructure into many cloud vendors [42].

Another incident has happened with Cloud Computing Incidents Database (CCID), where many cloud service providers experienced an outage from a couple of minutes to a couple of hours. The worst case lasted more than 24 hours of outage. Depending of the nature of outage and the affect that they cause on business performance while the cloud services access is not possible affects discontent to the costumer and loss of reputation. For instance, if the storage service is off then this will have huge impact on performing the computing service and the availability of the services.

The figure 13 shows an occurred outage with Amazon's AWS servers in Virginia

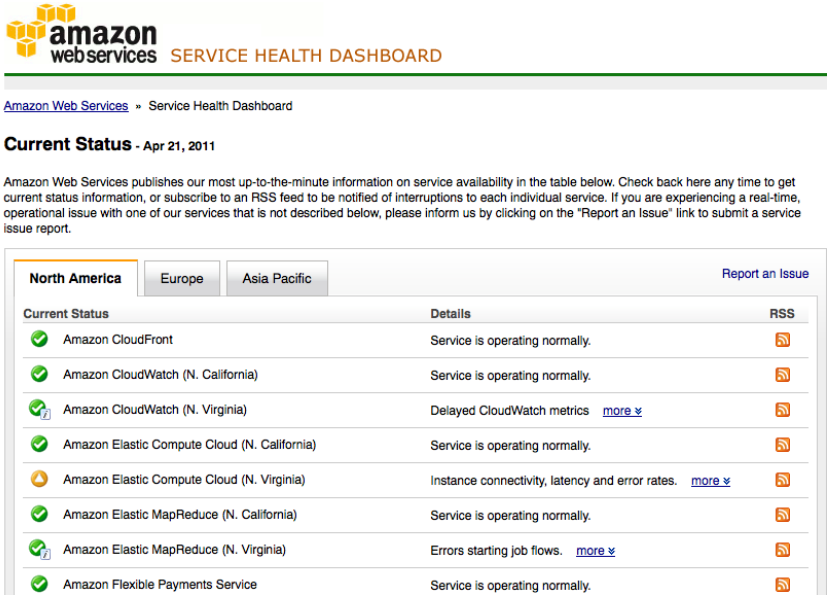

Figure 13: Amazon's Web Services outage [10].

The availability of cloud services depends from many factors such as provider's data center architecture, applications architecture, hosting location redundancy, difference between Internet service providers, and the architecture of the data storage. Below are presented some of the major factors:

- The architecture and redundancy of SaaS and PaaS applications.
- The architecture of the data centers, networks and systems including geographical diversity and architecture of fault-tolerance.

- Reliability and redundancy used by tenants and cloud service providers when the Internet connectivity takes place.
- The ability to react quickly, going through internal processes and procedures
- Users fault visibility, while in some cases when the incident is small and the impact of it affected a small number of users makes harder to take a picture of the impact and even harder to react and fix the problem.
- Trust and reliability of software and hardware features practicing on delivering cloud services.
- Security performance, network infrastructure, and their efficiency to face with a distributed denial of service attack.

Ability of security measures and processes to contribute on reducing the human error and protect the data from internal and external threats, e.g., users abuse with privileges. Cloud requires high service availability while operations should run into cloud continually and without disruption. However in case of incident events to continue with business operations should be a plan developed to act in such circumstances.

4.5.3 The Business Continuity Plan

Making a business continuity plan should include not only IT related concerns but also some of the key factors on performing good security in cloud such as personnel, facilities, crisis communication, and reputation protection.

According to [39] business continuity plan should include five phases:

1. *Analysis,*
2. *Solution design,*
3. *Implementation,*
4. *Testing,* and
5. *Organization, acceptance and maintenance.*

Disaster recovery planning is defined as a subset of business continuity planning and it performs based on processes, policies and procedures after a natural or human induced disaster [37].

Nevertheless, cloud is not a perfect solution for providing disaster recovery services. Incident management and disaster recovery processes are different for each company in traditional IT infrastructure, as it is in cloud infrastructure. Hence, every company has its own methods of managing incidents, making every cloud disaster recovery plan specific and different.

Moreover, to prevent incidents, companies should involve many procedures such as making policies, awareness training in such a way preventing human failures on educating users how to practice security measures into cloud. Data should be stored as well as into another data centre because in case of any kind of incidents, we need to have backups available.

Availability of cloud services has critical impact on business performance. Thus, it should be analyzed and have solutions in case of availability disruptions having the business continuity plan ready to use.

5 Market and Competition analysis between cloud providers

Virtual Desktop Infrastructure has ability to isolate specific users in case of individual incident without indicating into others performance. VDI requires a thin desktop to support storage space and running of the applications.

VDI performs security for companies through regulations and procedures having the focus mainly in security of virtual machines running within a datacenter and not so much into security of devices where the virtual desktop runs, however the health of devices is important because if the device gets infected there is a possibility to affect the security of user's virtual machine images. Moreover, even the computer is not well protected and well managed the user may have full access to the application, while the integrity of the data should treat and protect in the data center by the virtualization systems. Hence, the main concern regarding to the security is the protection and well management of the data by the provider in the data center, but also another important security indicator is the user.

VMware as one of the leading VDI providers makes possible to use virtual desktop using any operating systems by optimizing the computing resources based on users needs [28].

In some way the success of VDI depends on the security and ability of the vendors to prevent potential risks and their capability to design solutions. Most of the important issues regarding to security that the new technologies should integrate as a solution are: security of endpoint, application isolation, prevent data loss, runtime configuration, compliance and identity management with virtualization managing layers.

Moving to a virtual infrastructure is not an easy decision; the company should carefully treat the services and strategies offered by vendors, and adapt the appropriate one fulfilling its needs. Comparing three of the biggest virtualization vendors VMware, Citrix and Microsoft, we are going to focus more on the virtualization market, its priorities and strategies used to reach their goals.

The process of analyzing the market of virtualization providers may include the largest vendors such as VMware, Citrix, Microsoft, Red Hat, and Quest Software but also some of the smallest vendors such as Desktone, MokaFive, Virtual Computer, Kaviza, Unidesk, and Wanova. In this aspect, has been working the International Data Corporation (IDC) [1] which is a provider of market intelligence regarding to information technology and telecommunications.

Treating and analyzing all of these virtualization vendors helps being unbiased of each vendors strengths and weaknesses, thus making possible for the buyers to have information about the vendors and chose the appropriate one based on their requirements. The IDC analysis has been done by providing discussions, interviews and surveys with participants, users and market leaders.

[1] IDC's official website: http://www.idc.com/

5.1 Assessment of Virtualization Market Vendor

The vendors assessment was build based on two major categories such as capabilities and strategies. The main area of analyzing was the vendors capabilities to execute its own chosen strategy in the market and also the strategy of the future planning by them.

In the figure 14 is presented the position of each virtualization vendors. Market share is presented based on the size of the bubble [11].

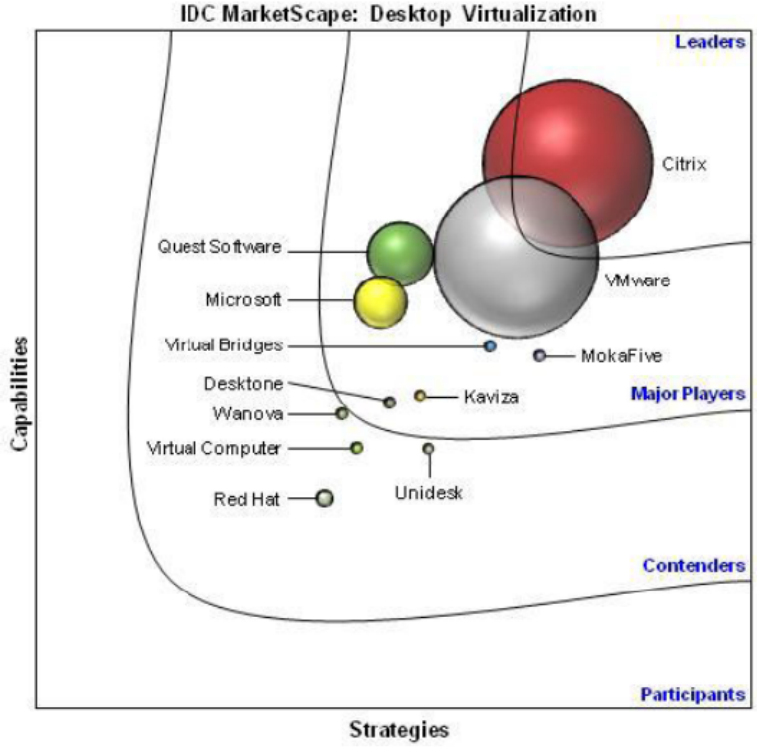

Figure 14: Assessment of Virtualization Vendor's [11].

5.2 Citrix strategies and improvements

As it is shown in the figure 14 Citrix is considered as a market leader in the server-based client computing. Recently the usage of Citrix has been growing taking the position of being leadership in the market of virtualization by making a lot of improvement in XenDesktop capabilities and in marketing strategies.

Citrix provide desktop management supported by the work of expertise, and special strategies for building a strong ecosystem, moreover making a strong partnership with Microsoft gives more power to be able to fulfill most of the costumers requirements. Citrix has developed a single solution of delivering Windows, Web, and SaaS applications to costumers, all with a common interface. Another positive issue made by Citrix is the possibilities for offline users to work without having the need to be connected anyway, but the centralized management accomplish the process of users' work when the is reconnected to the network. Citrix is considered to have

the appropriate strategies for deploy a virtual desktop infrastructure.

IDC [11] claims that Citrix has "*a good road map and a firm strategic grip on where it wants to take XenDesktop*."

One of the management members of Citrix declared [43]:

> "*We want a strong ecosystem. We want to enable choice.*"

This approach may be either good or not depending on the costumers business priorities. Citrix is known as supportive of multiple ecosystems. Building such an ecosystem is a good strategy, but still it does not have any big indication. They claimed that hypervisors are going to be the core of servers. Citrix claim also about their contribution regarding to the application lever, delivering the application regardless of what is needed from the infrastructure. This makes the operational and end user experience to perform better.

5.3 Microsoft's virtualization strategies and improvements

The director of Integrated Virtualization Strategy for Microsoft [43] claimed that:

> "*Virtualization is like TCP/IP. It's a means to an end.*"

Moreover, Microsoft supports the idea of that the hypervisor technology will be one day a commodity and uninteresting.

It is already known that Microsoft products are well supported by most of the users and they are satisfied with those products even if there is any better alternative. However regarding to the virtualization they admitted that Microsoft it was not a strong option for virtualization, but they became much better and claimed to be one of the leaders on Virtual Desktop Infrastructure.

5.4 VMware strategies and improvements

VMware is considered as one of the most successfulness providers in hybrid cloud by the company called Taneja Group [2], which works with analyzing and consulting for technologies and for the storage industry [44].

Hybrid cloud includes IaaS, PaaS or SaaS. Based on their research they claimed that VMware is the only provider that supports the industry leading virtualization combined with management solutions. VMware offers good performance of availability, compliance and security required in large scale deployments. VMware dominance of the market is as a result of management suite giving a strong advantage to this vendor.

Recently Microsoft is growing its market and expanding management abilities, but still there are some weaknesses in the architecture of Microsoft's virtualization platform and its security.

Security should be treated as important issue from all vendors. Comparing with other virtualization platforms VMware provides better security management through VMware vShield and vCenter. Amazon was estimated with good security management and features that would be expected from any public cloud providers. Otherwise, high score is given to IBM for their compliance capabilities, but they have been underestimated for their low virtualization security

[2] http://www.tanejagroup.com/

and for not being aware regarding to it. Security consulting, data management technology and virtualization management would indicate on performing strong security [44].

5.5 Advantages and Disadvantages of VDI vendors

5.5.1 VMware evaluation

VMware is considered one of the leaders on providing virtual desktop infrastructure, accomplishing its services at every level of the cloud market such as IaaS and management, PaaS and SaaS. The evaluation was made by analyzing the virtual infrastructure, network and storage resources, providing security into network, endpoint, application and user through integrated security framework. Connector makes possible for the user to move quickly their application from internal data center into a private or public cloud.

- **Advantages:**
  - Providing cloud IaaS and management, PaaS and SaaS
  - VMware establish better security by vShield security into the virtual desktop infrastructure by performing security at all levels, including endpoints, network, application and data.
  - Workload portability and interoperability platform, management, and security layers.
- **Disadvantages:**
  - The development of applications in .NET platform is not supported by Cloud Applications of VMware vFabric.

5.5.2 Microsoft Evaluation

Microsoft's VDI makes possible to access remotely to the desktops and applications by authorized users and devices. VDI is considered to be the best way to deliver application claiming to have high security performance, even whether using unmanaged devices [45].

Main overall advantages of Microsoft VDI are defined as follows:

- Microsoft is providing to the cloud market all models including IaaS, PaaS and SaaS
- Microsoft is using a lot of recourses on educating and training its cloud partners and customers to deploy centralized desktops in order to get more opportunities.
- Establishing VDI and going beyond VDI.

On the other hand Microsoft has some disadvantages regarding to other competitive providers.

- **Competitive Disadvantages:**
  - To provide hybrid cloud Microsoft started relatively late. It was claimed about the lack of security, network and storage in the private cloud
  - Capability to enhance the virtualization market is still closely connected with windows server and system center.
  - Microsoft is considered with fewer capabilities on IaaS then in PaaS.

To analyze any VDI provider in general is quite difficult and requires a lot of time. Hence, the

access workflow and policy enforcement of VMware and Citrix is presented briefly as chosen example.

5.5.3 Citrix XenDesktop

The policy enforcement applied in the data center for Citrix XenDeskop is presented in figure 15.

- Users may access to XenDesktop from different devices using the web interface.
- Each user access his virtual desktop.
- After being accessed to the appropriate virtual desktop the user is pushed to the Enterasys DCM (Data Center Manager) solution.
- The Enterasys DCM solution makes the segregation of each virtual desktop through policies in order to set the user into his virtual desktop.
- Virtual Desktop helps to access resources in the infrastructure by the users. Rules for access control and Quality-of-Service issues are applied by the virtual desktop.
- The network administrator has abilities to identify the login users, their profile and all virtual desktops.

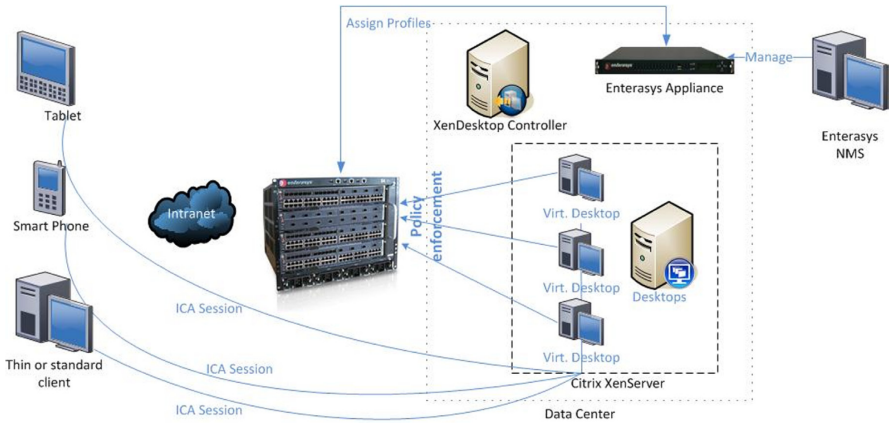

Figure 15: The applied policy enforcement for XenDesktop [12].

5.5.4 VMware View

This section describes the policy enforcement applied in the data center for VMware View [12] as it is presented in figure 16.

- Through thin desktops users may sign into VMware View Manager.
- Each user is having their corresponding virtual desktops.
- After being logged in into their appropriate virtual desktop, the virtual machine is connected to its datacenter network using 802.1x EAPOL messages.
- The Enterasys DCM solution provides the appropriate profiles and policies for each virtual

desktop based on users privileges. Enterasys NACNG makes possible to control access.

- Virtual Desktop helps to access resources in the infrastructure by the users. Rules for access control and Quality-of-Service issues are applied by the virtual desktop.
- The network administrator has abilities to identify the log in users, their profile and all virtual desktops.

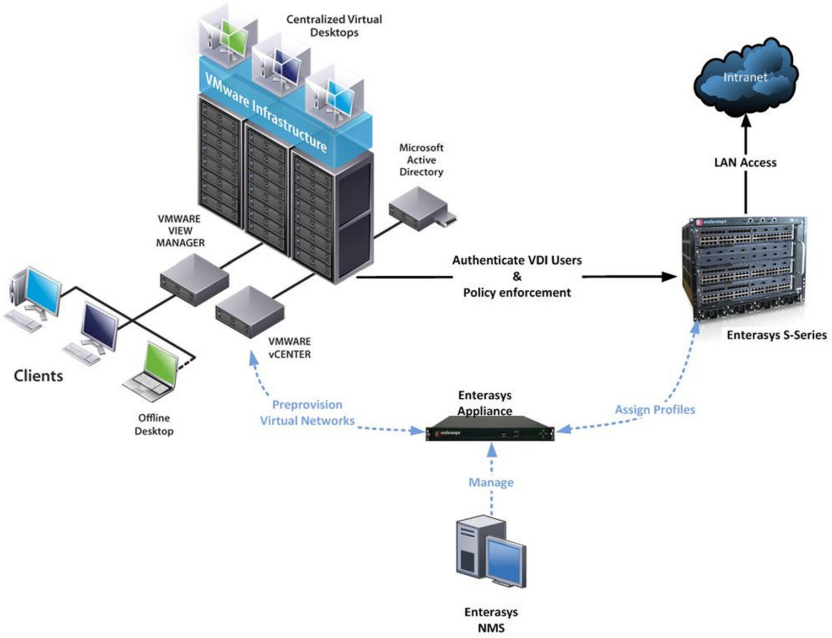

Figure 16: The applied policy enforcement for VMware View [12].

5.6 Features Comparison between Virtualization providers

Understanding features comparison between VDI providers it is considered as important issue, especially for companies planning to use one of the services offered by virtualization vendors. Most of the VDI products have its own functionally and features set, and it is important to have an overview of the solutions, functions and services offered by them. In this point should be vigilant and analyze them well, while some of the providers are specific and easy manageable but there are also providers that provides services in a bit more complex way. Thus, some vendors are focused more in offering complete sets of functionality, while some of them are focused on providing small solution but with specific functionality. Both of the scenarios are good options, just depends on the costumers functionality needs.

In Appendix B are listed some of the main features of three main virtualization providers Citrix, VMware and Microsoft, their solutions and functionality on a high level offered by them [12].

To find the best VDI platform is not easy while it depends on the costumers requirements

to find the appropriate platform which fits with their needs. Thus, without understanding the requirements in deep it is hard to suggest any of these VDI platforms. To analyze each of these providers and chose any of them depends on the evaluation of the vision and strategies around Application and Desktop Delivery model. Using the right technologies, designing, building, managing and maintaining the VDI it is an important step Phrase regarding to "VDI fits every customer, but not for every desktop".

6 Virtual Desktop Infrastructure and Security issues

Companies have the possibility to evaluate the risk of virtualization technology models before adapting their services rather waiting too long of treating the most important requirements. We describe how to treat the risks exposed by VDI, by exploring and investigating three main factors on VDI security performance within the organization:

- **Technology**
- **Processes** and
- **Human aspects**

The project will cover the analysis of security issues regarding to VDI. One of the most basic mistakes that people do is treating information technology as just technology approach. Thus, this is of course a failure of people behaving in such a way, causing to the company security events, damage and cost. Regarding to this issue, based on researches that are done it is obvious the need to investigate not only the technology but also processes and in particular human aspects as one of main indicators on security performance.

Organizations doing mistakes on treating this concern as technological problem and adapting technical tools instead on adapting strategies and regulations based on risk management concepts.

Organizations should be aware and informed about benefits of using cloud services, however, they should be more aware about the potential risks and implication that the company may face when virtualization infrastructure is used. Hence, the company should analyze two main factors such as cost and adaption risks.

To prevent any undesired issue when the company is planning to integrate cloud services and virtualization technology first need to analyze and make risk assessment before taking this step. However, most of the companies are realizing that cloud services adoption is a need and its time has arrived, but their challenge is to update security strategies to make easier its adoption. Another important issue is that organizations are not alone dealing with these security concerns. There are many agencies dealing with these issues such as Cloud Security Alliance (CSA) [1] and ENISA [2].

Making risk assessment is very important to include challenges of VDI but also the benefits of it, the efficiency indicator to employees working processes and the companies' gains. Hence, this is the best method to identify organizations needs and potential risks from the beginning, which helps to understand the related risks and prevent or improve the performance during or after the adaption.

[1] https://cloudsecurityalliance.org/
[2] http://www.enisa.europa.eu/

6.1 People as a security indicator

6.1.1 Training and education

Most of the organizations pay attention only to technology at the detriment of people, training their employees well about the new applied technology in order to understand and get knowledge for any changes in process given by the new infrastructure.

Thus, training procedures have critical indication on educating staff within a company such as training administrators, operational staff, solution architects, and users.

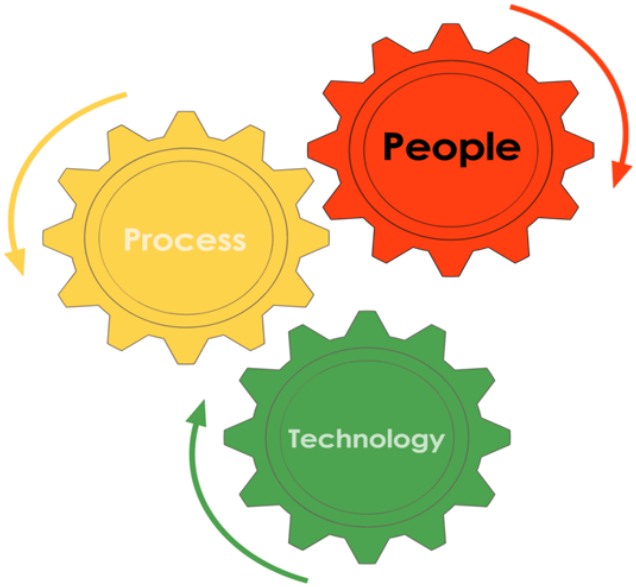

Figure 17: Three pillars of information security: **people**, technology and processes.

6.1.2 Human factor

The impact of virtualization infrastructure on employees working processes had been apparent. Using cloud services is very common and widely used, so it might have impact on the manner that people are living and working with, in terms of the data location, the way that IT systems are integrated and the process of data transfer. The impact of Cloud services in risk profile and users lifestyles and also in the working process will be depended by the method and the way of cloud provided services [46].

6.1.3 Risk awareness

To increase the security performance about cloud services and VDI is needed that employees to be aware of information security risks and also the importance of protecting information because of the increase of sharing information. The possibility to access corporate recourses by VDI should make the employees more aware about possible threats; accessing process may be looked from any other person. A big threat is considered the ability of looking to the screen when the user attempts to have access to the company systems and resources. Organization using an in-house

computing environment and then moving to the cloud computing infrastructure exploits a lot of security issues and particularly a big challenge is policy and enforcement data security on shared and third-party which makes cloud policies and awareness much more complex comparing with traditional IT environment. This indicates on having information where the cloud systems are exposed to users (i.e. data sharing or application supply)

To perform desired controls in the cloud, the company should make a step-change in the level of awareness, care and classification of the information and security among its staff. However, even the company is having support and control performance over the virtualization infrastructure by the cloud provider, still the company need to recognize that this may be not enough without treating the role of the user in classifying and protecting information.

Based on confidential information levels, organization has the ability entrust to the cloud and to decide how the cloud services are integrated with IT systems.

- Users education about how VDI works and information related to its usage.
- Levels of care that should be applied the security for that information. This may be helpful to develop and create rules performing metrics and behaviors within a company.

VDI indicates on the business performance and its staff wanted to have access to the systems and data from different location outside of the company by different type of devices, and also another issue is the ability of sharing information easier with third parties, thus, awareness would be a proper method of educatiton.

However, despite of benefits offered by virtualization technology there are some other concerns regarding to this infrastructure such as data security, availability and compliance.

Adapting VDI by the organization bring new challenges about how to ensure:

- *Security and privacy*
- *How to achieve balance between security and cost-effectiveness,*
- *How to increase the availability of systems and,*
- *Treating the presence of exit strategy.*

Thus, to prevent incidents caused by various reasons even by cloud providers itself, the company need to consider seriously possible security events, making data classification and analyze some issues such as what information and business processes may run into the cloud and what information to keep inside the organization. It is hard to apply this method of prohibiting sensitive information over the Internet when business processes relies exactly on that. Business issues related to people and organization and also the risk environmental are very important for security performance into cloud.

6.1.4 Policy challenges and indications in human behavior

Changing the employees' methods of working is not an easy task; this brings many challenges on human aspects. People used to work in some additional way using a variety of devices, connecting remotely to enterprise resources and then changing the corporate guidelines in terms of IT usage and data security, provide policies, change standards and procedures of the corporate, and make possible to be followed these procedures by the employees is very hard. This concern

will increase over the next years. It is evidence that this generation and even more next generation of employees are growing their activities using online communities, sharing the data and application over the web, thus they are having less concerns about the corporate standards in particular areas such as data management. Employees also want to have access from different devices chosen by them and with no limitation about access location to the corporate network.

To have control and to change the attitudes as David Lacey said in his book "Managing human factor" is very difficult.

"*Changing People's level of knowledge and awareness is major challenge. Transforming people's attitudes and behavior, however, is a much more complex task, especially across a large, conservative organization.*" Thus, to help on managing attitudes regarding to data security access, and provide support for accessing the network by non corporate devices, organization should develop special training for their employees including security training and awareness which contributes on raising the knowledge of security into cloud. Awareness program may involve security concerns and challenges in order fulfill with organizations requirements and behavioral standards [46] such as:

- Place controls at the device level.
- Define the types of information on the employment contract that may be stored.
- Define Security rules of sharing online information in the cloud.
- Conduct an assessment regarding to the location where the data are stored.
- Define possible implications for regulatory compliance and possibly employer/employee relationships.

Risk management is important for information security but still there are many other factors including:

Functional requirements include some of the security features such as access control and identity management.

Commercial considerations involve security features that may be integrated in some of the products and services, growing the sales in markets that adding a high value on security.

Corporate policy includes rules and political requirements. This mostly reflect organization culture, based on historical or security risk of the projected levels

Legal requirements provides the issues that the organization should apply such as data protection and copyright legislation.

Understanding security risks dealing the users with, and the way of implementing the corporate security policies has become really imperative for most of the organization. It works better if the managers and all the staff appreciate the importance of virtual desktop security, practicing security measures also beyond corporate boundaries. Human factor had been always considered as a critical factor on security performance but using cloud services has grown even more its importance because of the possibility of accessing to the corporate data out of the company anywhere and anytime. To make people going through policies and procedures is not easy, usually it is not impossible to get applied successfully. Most of the people do not have the willing to follow policies and procedures, but still the corporate governance should make rules for its employees

to make them going through provided regulations and policies.

According to David Lacey (page 134) [47]:

> "*people are different and they have different attitudes influenced by culture, age, gender, personality, pressure, lifestyle and many other factors and this probably indicates on not having the same influence of the policies to the people.*"

Policies may be another issue that would help on convincing companies to adapt cloud services. Moreover, through policies companies may realize the benefits and reduce their worries and concerns of providing this infrastructure [48].

6.2 Policy suggestions for changing humans behavior

The scope of policies is to introduce security methods when using cloud, information transfer and human aspect in respect to security performance. This could be applied for the whole virtualization infrastructure. Purpose of these policies is to make users under a controlled environment and get informed about their responsibilities, communicated policies regarding to what processes are not allowed in order to prevent a disclose of organizations information.

- **Users should be vigilant regarding to the environment circumstances when working and accessing to the organizations data through cloud infrastructure.**
  As it is described several times in this project, cloud usage has its own benefits and one of them is accessing the data even if the employees are outside the company boundaries. However, this has also its own risks indicating situations to happen that someone behind the user monitors users screen and read its content, either deliberately or not. The perpetrator may catch even access credentials such as username and password, furthermore, catching confidential information casing several damages to the company. Nevertheless, catching the information through watching into screen depends on the duration period of watching and environmental circumstances.
  There are many devices that cloud record the work process into cloud and as a result catching access credentials and also getting information that could be important and sensitive. Thus, environment has importance and companies should define places where the access is not allowed such as bus and train stations, cafeteria, and parks, mainly where the amount of people is high.
  However, depends of the company willing and standards but working in public places can be used tools such as screen filters making readable the screen only for the users working in front of the device and making the screen dark and unreadable for the people being a bit far from it. Developing awareness program and including this kind of threat may be very helpful to make people aware of facing with this issue while people behind them might be a really threat to catch various sensitive information. For instance, some data privacy regulations specify that data can only be accessed in certain geographic locations.
- **Lock the computer when leaving it, and do not leave the computer unattended being outside the company.**
  Leaving the computer unlocked and going away even for few minutes would indicate on get-

ting people around you curios of checking it, and this could have as e result stealing information and data related to the company which would be either to sensitive or not. However, the case would be worst if the computer is left unlocked when being out of corporate walls. People easily can catch information from unlocked computer using memory drives and the owner may not even detect that any incident has happened.
However, leaving the computer unattended (but locked) on working environment does not appear the same risk as leaving it outside the company while working in public places. In this case are needed few moments and the computer probably would be stolen. Even the computer has been locked there are possibilities to unlock it and find in some way the access to VDI by finding users credentials and as a result getting access to the important data and the case would be even worse if the hard drive and information's are not encrypted.

- **Encryption of the sensitive data.**
  Moving sensitive data into the cloud infrastructure may cause new security concerns and privacy threats. Thus, privacy of the data but also its confidentiality and integrity is protected through encryption process. Even the data are encrypted it does not mean that are fully protected, there are several techniques that could be used to decrypt the data content, but this is a difficult process and normally encryption is much more secure than having the data unencrypted. The encryption process makes possible to be data transferred in the way that an attacker cannot understand. Anyway, when data are encrypted never store the encryption key in the same cloud storage.
- **Never give away username and password and do not share information with anyone.**
  In cloud infrastructure the access credentials are very important and have critical impact. Thus, sharing username and password with anyone else is prohibited. Sharing the username and password with other people means that they will have all the information that could be sensitive and very important for the company. This would have many consequences regarding to the data privacy, data disclosure, data integrity and confidentiality and many others.

6.3 Pocesses

6.3.1 Addressing Liability and Regulatory Concerns

In certain cases, moving the data from an internal network to the cloud based infrastructure may be faced with uncertainty laws, regulations and potential liability causing challenges regarding to cloud services usage. Issues regarding to the governance with data security and location makes complicated the process of ensuring compliance with the law. However, companies are concerned about the security of their own data, if the company itself is not directly connected on managing it. Sometimes, legal issues may be an indicator of having hesitation moving toward cloud infrastructures, but even cloud providers deal with the risk of liability and regulations, reducing the number of cloud services offered by them. Thus, laws define strict rules about particular issues, for instance, laws defining that particular data are prohibited to be stored abroad, making more complex this task for cloud providers.

Cloud providers would not be able to offer services without accomplishing processes [48] defined by law.

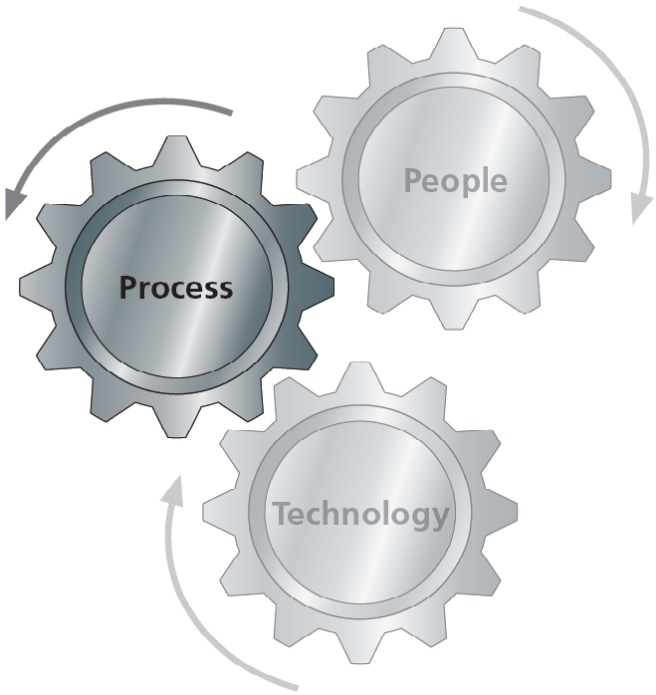

Figure 18: Three pillars of information security: people, technology and **processes**.

6.3.2 Following legal recommendations

The decision pro using cloud services start with contract evaluation.It is common to analyze the market issues assessing contracts and SLA (Service-level Agreement) offered on the market. Cloud services as a business model is not the same with outsourcing, using these services by offering to its costumers a lot of benefits such as low cost and commodity service. This process makes possible to assess the security risks by both costumers and cloud providers. However, there are many issues that in certain cases should be included in the contract and treat very well including rights and obligation regarding of getting notification of security breaches, data transfer, change of controls, and data access by law rules. Thus, costumers and vendors should focus more on addressing the security risks in the contract agreement while the law will support in terms of data security and accomplishment of that contract in a proper way. As presented above there are many issues the should be treated in the SLA and other forms of agreements when transferring to the cloud infrastructure:

- **Data Protection** would be achieved through technical and organizational security measures ensuring the processes to be carried out and compliance.
- **Data Security** includes security measures that should be used by costumers and cloud provider in order to prevent any incident otherwise they would face with regulatory and judicial measures if the procedures addressed in the contract were not followed.
- **Data Transfer** would treat information that could be given to the costumers regarding to the

processes of data transfer within the cloud provider, outside of that cloud and for instance the transfer inside and outside of European area.

- **Law Enforcement Access** treats the unique rules and regulation regarding to data access. The costumers should carefully analyze the information available provided by the cloud provider regarding to the jurisdictions of the data stored and based on this to evaluate any possible risk resulting from jurisdictions which may be applied.
- **Confidentiality and Non-disclosure** is a critical issue which should be carefully reviewed to prevent security incident related to data confidentiality and its disclosure.

6.4 Technology

6.4.1 Lack in isolation of resources

Computing resources of a particular user can affect other user's resources. IaaS infrastructure works with physical resources sharing in multiple virtual machines and offering these virtual machines to multiple users. Potential vulnerabilities in the hypervisor security may cause security breaches in causing unauthorized access. An example could be, two different users (costumer A and costumer B) have their own virtual machines and their virtual hard drives placed in the same shared LUN (Logical Unit Number) stored inside SAN (Storage Area Network). The costumer A would be able to map the costumers B virtual hard drive and be able to see the data inside it. In the Hypervisor security model existing any possible vulnerability would indicate on leading unauthorized access into user's data. This kind of vulnerabilities can cause several security issues by manipulating user's data and launching different types of attacks such as DoS attacks, data leakage, comprises of data, or any direct financial damages. Moreover, the lack of different approaches to enforce the quality of service or by being more specific in SLA, providing better quality of service (QoS) or distributed recourse scheduling (DRS) products, may indicate on allowing a user to monopolize the cloud usage facility, causing disruption into other costumers work by launching denial of service or impacting a poor performance [49].

Usually, cloud costumers have the lack of knowing the risks that they are facing when moving into the cloud, specially for specific threats, for instance loss of control or vendor lock-in. Dealing with this lack of awareness will have impact on affecting cloud vendors to not have the sufficient knowledge regarding to the action that should be taken in order to mitigate these risks.

Virtual desktop to have better security performance must pay attention to it. Most of the time the protection is much easier when virtual desktop is used, because the images are stored in a datacenter and the working performance is surrounded by the organization security tools such as firewall, intrusion detection and prevention systems. Nevertheless, the security of individual virtual machines has its importance. There are many opinions especially from the users side that they do not need security tools like antivirus or antimalware programs on their virtual desktop. But still there is an operating system taking place. In case of users infection either by a malicious webpage or getting a virus through email could be affected the individual virtual machine images. The purpose of security tools is to protect the images of becoming infected, in this case even the process for remediation may be much faster comparing with traditional desktops.

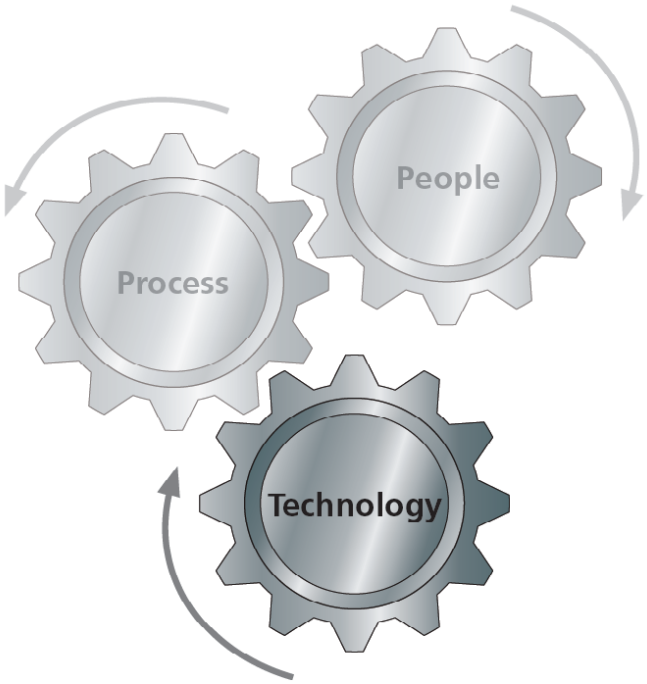

Figure 19: Three pillars of information security: people, **technology** and processes.

The process of remediation depends on the user's profile and their working process. Some virtual machines may become uninfected using the method of being turned off and on again and after the reset is done the infection will be removed successfully. However, the case is different when organizations for its employees accessing remotely from different location and accessing to the datacenter where the security level is very important. This includes both processes the connection to the datacenter by the users as well as the protection process of the datacenter against any possible attack coming from endpoints that are not managed by the company and became infected. Mostly the enterprises use IPSec or SSL VPN to get access and protect the connection between firewall and endpoint. Users usually are required to install VPN client in their devices. Companies may perform better security through demilitarized zone (DMZ) in place and proxy the user across, making user in contact with the datacenter not in direct mode.

6.5 Addressing Security Threats in Cloud Environments

This chapter outlines some of the main security threats into cloud environments that companies are facing with. Confidentially, Integrity and availability usually is a combination of security performance. There are many detailed security threats that cloud services are facing with [50].

Risks are present as a result of many factors such as data location, data segregation, privacy, lack of knowledge about the policy governance, insider threats within a company and some others. These are the most common risks that companies are facing with and are going to be treated in this project. Thus, when virtual desktop is used by the user which is utilizing some

resources that could be defined by the provider regarding to the decision if that particular task is going to be executed and when these resources are going to be released. Hence, this process flow is provided by the provider and not by the user causing a big challenge regarding to the users data security, integrity and privacy [14].

6.5.1 Malicious Insiders

Malicious insider could be much more dangerous than other types of attacks. The impact within the organization would be in the data confidentiality, integrity and availability including all the types of data and services. Thus, this would have as an impact reducing the organizations reputation and shaking the costumers trust. Such issue should be considered because of the importance of certain people's role having in cloud infrastructure indicating on being factor with high risk profile. These people could be system administrators, people working with intrusion detection reports and incident response team. While the usage of cloud service is increasing every day meaning that employees are becoming very attractive target to be attacked [49].

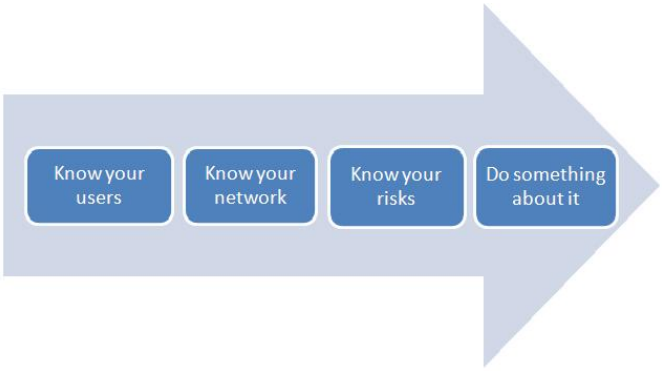

Figure 20: Treating insider threat [13].

Insider threat is treated from many years ago but now it is considered more critical than never before. Hence, companies hiring people should carefully treat this issue because of the possibility having access into many sensitive data, if the insider threat exists then various sequences are in place such as stealing important information, disclosure of them, and many other malicious activities. Before hiring working staff the company is suggested to make review of historical background one of the checking issued could be if the person had any kind of criminal experience or did s/he has been faced with law punishment, in other word to be reviewed most of the activities for the person that the company is planning to hire.

6.5.2 Threat of data loss and leakage

The loss of data happens when another person is having others data that could be sensitive or not. Thus, one choice of protecting these information could be the performance of data encryption. Since, the data leakage may happen more often when no secure software keys and weak authentication process is used. Incidents as a result of unauthorized access to users' accounts are becoming common activities because of using weak access controls for virtual desktop. Hence, these vulnerabilities and weaknesses could be repaired through very well education users and

staff, through policies and awareness in order to provide information regarding to the importance that they are having in protecting their own and organizations data. Another more technical threat is considered the data transmission attack, where the attacker is launching an attack in order to get network access through spoofing. Since the hackers do this by monitoring the users' network and in some way using various techniques achieving to get information [51]. Providing

Figure 21: Top Reasons of causing Data Loss.

virtual desktop infrastructure means that the technology is shared. Hence, data should be adequately segregated to ensure the data access by the right user, in other word making sure that each user is accessing to his/her own data without affecting others data.

Better security performance is achieved through [51]:

- Encryption and
- Digital data signatures

Applying data segregation in cloud infrastructure is not easy at all; it can face with the lack of doing this process based on users needs. There is also another issue regarding to encryption making some costumer to not apply this technique because of the possibility of being destroyed the data as an indication of encryption performance.

The Data might face with both internal and external threats. There are possibilities that the attacker would hack the users' hypervisor and the shared CPU, reaching at the attack point of manipulate, delete or destroy the data. Nevertheless, data encryption is one of the important issues when it comes to ensure data protection from being hacked or attacked. Even more encryption is needed to take place for sensitive data but this requires other resources and one of them is the increase of cost. In the table 2 are presented some of the security mechanisms provided by most

of the cloud vendors [14, 51].

Table 2: Security Mechanisms provided by Service vendors [14].

Security Issues	**Results**
Password Recovery	90% use common services 10% use sophisticated techniques
Encryption Mechanism	40% use SSL encryption, 20% use encryption mechanism 40% utilize advanced methods like HTTP
Data Location	70% of data centres are located more than one country
Availability History	40% indicate data loss. 60% indicates data availability is good
Proprietary/Open	10% have open mechanism
Monitoring Services	70% provide extra monitoring services 10% uses automatic techniques 20% are not open about the issue

To protect the data in transmission it is used Secure Sockets Layer (SSL) but most of the data storage is in a shared environment. People are not that much informed but they usually think that the data security is performed when the key length and encryption algorithm are used as strong as possible, but this does not mean that they are wrong and these two measures has really good indication on performing better security. However, these techniques could have also complication; the most likely one is the failure and mistakes in implementation and as a result getting exploitable weakness.

Security performance [27] in such circumstances would work better if:

- The encryption implementation is designed and tested by experts in this area.
- Have knowledge about who performs the protocol and code reviews.
- Get informed about who knows and who has access to the decryption keys.
- And who is having access in case of emergencies

The performance of these security measures applied in real life would work well and the chances to get data disclosure are much lower. Treating these issues and human aspects would help in some way to prevent security incidents.

6.5.3 Privacy Risks

Privacy is a core issue for security in the cloud. Most of the companies are not comfortable with the storing application and data into another place outside their on-promise datacenter. Moving too many information to the cloud makes cloud costumers worried about data security, privacy and potential unauthorized access. Cloud vendors must assure their clients that they are providing a high level of transparency and privacy performance.

Privacy risks in cloud environment involve many different risks. The most basic issue regarding to this is the lack of existing laws to block the disclosure of information to the cloud providers. Information disclosure may have serious consequences, while many businesses do not want to share information with third party, but this kind of information are stored into cloud and would have possible impacts on business functions. Therefore, before using any of the cloud services and storing information on it, is highly recommended and important to understand the Terms of Service (ToS) and the Privacy Policy of the cloud vendors. However, in case of not being able to understand the policy or in case of not offering the appropriate service required by the costumer, the user can switch to another cloud provider getting the appropriate service.

Organization always should be vigilant on analyzing the privacy and confidentiality aspects into cloud environments [14, 52].

There are two different cloud structures used in cloud environment using different privacy settings for each of them:

Domestic cloud leads the usage of the cloud located physically within the same location. Leading the possibility to raise the privacy issues such as getting information about the possibility of data collection, usage or data storage in the appropriate way and getting information when the data is disclosed to authorized receipts only.

Another issue in the domestic cloud infrastructure is the rights of the owner to access their data. Hence, the manner of accessing the data by its owner should be well defined. Privacy issues may be extended to all cloud environments in general way [14].

Trans-border cloud is a structure where data are transferred across the borders, causing more privacy issues. Specific and strict rules could be performed when transborder is used for data transfer based on the data location. This kind of infrastructure is used for data governance based on location, for instance several European countries have particular data that are not allowed to go beyond their borders; these procedures are applied in many countries over the world. Many of the countries have strong rules made by their government [53].

6.5.4 Data Location

Cloud providers usually are not concentrated in one particular datacenter but they are using more than one datacenter in different countries for storing client's data. This makes cloud costumers concerned regarding to the stored location of their data. Data stored in multiple locations could have impact on hindering investigations within the cloud making much more difficult to know the running activity. Dealing with organizations sensitive data in the cloud should make aware both parties to go through contractual commitments [14][51].

6.6 The newest challenge of VDI - Bring Your Own Device

One of the current and upcoming trends in IT is Bring Your Own Device (BOYD). The term requires many changes in the way of using devices into the workplaces. BOYD is making possible for the employees to choose their own devices indicating on increasing productivity and mobility. This kind of devices may be provided by themselves or by the company. In the future is expected the usage of a single device for many purposes: computing, communications and running of applications. However, there is a possibility of using different devices for different tasks, for instance people mostly use phone devices for mobile communication even having a laptop. Thus, people are going to use multiple devices for their tasks instead of using a single device for all purposes [54].

6.6.1 The role of VDI into BYOD security

Connecting to a virtual desktop session using any kind of mobile devices makes running applications to be executed in the data center. Hence, organizations and in particular the IT department have more control over the running applications and operating systems as a result of not running and executed directly on the devices. To achieve better security performance using BOYD, the organizations need a client component in order to connect users to the VDI. The usage of client component need to be approved by IT department in order to make the connection much more secure and provide protection against data leakage.

VDI makes possible of addressing some of the external threats including viruses or malwares and provides data security in case of stolen or lost devices. Providing data access controls helps on preventing data leakage, this could be achieved by BOYD policies determining place and time for data access. An example could be policies and rules for delivering emails to an external account.

Treating human aspects and their behavior when using BOYD makes companies much more concerned about. Moreover, users usually try to ignore security policies and the organization should have always this aspect in mind. It is not just enough developing policies but they should make the situation to be followed by the users. Organization's technology and its management should be aware of the possibility that users may find solution to bypass security measures and controls.

6.6.2 Management of mobile devices with VDI and its challenges

Usage of mobile devices and their management sometimes is difficult. Usually most of the organizations use virtualization platforms (i.e. VMware View) to make possible for their employees the accessibility on different devices. Nevertheless, challenge of BYOD regarding to its management are human impacts, so the organization must educate user when connecting to virtual desktop, use of appropriate hardware and enforce BYOD policies. Virtual desktop makes easier management of BOYD by making possible to manage the VDI session and application instead of using hardware. This new possibility has brought flexibility by providing services connecting to a desktop from any device, any time and from anywhere [55].

VDI provides application running in the same way by all users. However, there may be provided customization for particular users based on parameters of the application and setup, this does not indicate on hardware configuration or software requirements (server/client).

7 Case Studies (Interviews)

This section will describe the interviews results and security experts claims done during the project work. The flow of interview process started informing participants about thesis topic and then they were supposed to give their presumption in different cases regarding to the content of the topic. The questions were given to the interviewees in advance before having the meeting. Thus, they were aware of the content of questions. The approach of this was to get their opinion but also introducing the security performance in their companies. The interviews were informal, and with no limited time. The task was first to analyze the interviews and provide details in comparing the key findings and similarities, furthermore analyzing the results taken from the interview processes.

The Interview was conducted with the help of the following companies:

- **Microsoft** (Norway) [1]
- **NorSIS:** Norsk Senter for Informasjonssikring [2], and
- **ETAVIS GNS AG** (Switzerland) [3].

7.1 Case Study: Microsoft (Norway)

The study made with Microsoft had the purpose to provide information regarding to their VDI products, their experience in security and the priorities in providing security performance treating technology, processes and human aspects. The start is by giving an overview of security officer's task when using VDI, security measures used in outsourcing and human responsibility and treatment by one of the leading companies in IT such as Microsoft.

7.1.1 Security officer's tasks using VDI

Three of the interviews done in this project were aware of the importance of virtual desktop security. The question was to give the description of how the security officers task change when using virtual desktop.

There are several methods to implement virtual desktop. The options comes from the client side to choose the entire desktop virtualized or just to have some application virtualized claimed the Chief Security Adviser (CSA) at Microsoft in Norway. Microsoft as one of the leaders company has launched both of options. They are providing application virtualization platform developed which is App-V [56] and in other hand the Microsoft's Virtual desktop infrastructure is Hyper-V. The CSA of Microsoft in Norway claims that the main benefits of VDI are the amount of possibilities and the ability to have much more environmental control. However, the negative part is being limited in some particular areas and the lack of choices usage, but still enhance

[1] http://www.microsoft.com/nb-no/default.aspx
[2] http://www.norsis.no/
[3] http://www.etavisgns.ch

is used in virtual desktop. Providing these kind of services depends on the organization and roaming profiles whether is used remote terminal server session or remote desktop session the user is able to login into different devices with the same credentials and this is good way of working and has positive sides for both security and users experience background that could be important before using it.

Some of the challenges in cloud environment starting from mentioned and treated by the interviewee could be:

- Cloud management for private devices
- Optimization infrastructure for virtualization
- Unified management across devices (Smartphone, tablets, computers etc)

A Huge amount of requests is performed by these types of devices called consumerization [4]. Microsoft's employees use both of cloud services for file hosting, service SkyDrive [57] and SharePoint [58], but they provide different security measures while Skydrive is possible accessed everywhere having the same picture and the same resources but most of the SharePoint resources requires being in the circle using it just inside their network. This means that the company applies different settings when using these cloud services by its employees. Hence, the companies concerns might be when these services are done in both places indicating many challenges as unified management across devices.

Challenge is how the security officer or IT security department ensure that unmanaged devices are compliant, for instance if the devices are not carrying any virus, malware. Thus, with this issue Microsoft is working with, to check the health of device before using these services. Nevertheless, the health of devices it is known most of the time, knowing the types of application are running and many other details, but this kind of monitoring is a bit difficult when the process is running out of the private network. This difficulty is to make a choice of workloads.

VDI is very task oriented so the updates or to add another software would be harder, because to do it via VDI takes much more time and efforts, claimed the Microsoft's CSA. However, Microsoft is very concerned about PPI (Personal Private Information) such as personal sensitive information, making them to invest much more in this aspect as a company.

Main areas that Microsoft is focused more with are:

- Policy
- Roles and Responsibilities
- Training
- Metrics
- Reporting and
- Operations

Microsoft as a company is paying more attention to the people behavior more then never before, because based on their statistics 44 % of the incidents are as a result of

[4] http://www.microsoft.com/en-us/windows/enterprise/customer-stories/consumerization-of-it.aspx

human failure.

7.1.2 Security performance when performed Outsourcing

The company has strict rules making everyone having any kind of data to perform classification of the data through conditions such as data with:

High business impact: They are providing high protection measures for this kind of data, for instance source code, information of costumer's credit cards are classified as with high business impact. Thus, these data mostly are encrypted by internal security.

Moderate business impact: deals mostly with data confidentiality. Working in a project with another company as outsourcing means that before it starts to sign formal agreement, making very clear who is responsible and who has access to the data.

Sharing information is based on classification and role as important indication, for instance being a project member and moving or starting with another project moves also the employee's role preventing the information to be taken by that person.

Role and access indicates on preventing any confidential information disclosure, by making the company to provide features applied for the files in order to make impossible from being shared. Asked if any organizations member leaves the company and has the computer with all data on it, the answer came like this: accessing to the confidential data is based on access privileges and control. After leaving the company the username of that person is removed even if he is having that information in the computer he cannot open and check through it because connecting to the confidential information is needed the access permit.

7.1.3 Impact of security policies in the future

Data classification and protection are supported by policies meaning that policies have great impact in performing security. Regarding to the High business documentation the company perform strict policies, for instance high business impact documents cannot be stored locally but only through systems provided by the company based on Identity and access management rules and policies claimed the Microsoft's CSA.

Usage of social networks includes policies for human behavior, for instance employees are not allowed to talk or tell anything regarding to the products which are coming up or current ones. In addition, Microsoft is using a lot of policies regarding to the data security in the cloud when accessed by the user. Accessing to confidential and important information there are policies that should be complied, for instance the computer hard drive must be encrypted otherwise the user cannot access to the data except to some particular information such as email, user's profile etc.

Policies settings used for systems are performed only by the user's identity and access management. Based on user's ID is possible to do many services over Internet. For instance, for Microsoft's users to buy a flight ticket, is needed only the employees ID and connect to the private network and then to the vendor (business partners) ordering the ticket based on policies provided by the system and based on users identity and access management. This procedure is based on the internal policies provided by the company (Microsoft).

7.1.4 The Future market share of new Computing (VDI and cloud services)

In the future, based on the opinion of the interviewee, there would be much more system like that one mentioned in previous sub-section 7.1.3, where people will use cloud services just based on their ID and access to the services chosen by them self. Currently, not many business companies are using this kind of systems and infrastructure. In addition, this kind of collaboration between companies will be increased, sharing information and providing better services for users.

Regarding to the privacy when sharing this kind of information will include some information but not everything. All of this infrastructure will be hosted in the cloud. Security measures would be applied depends of the location or what kind of data are handled. However, very confidential data will be stored in VDI environment in virtual machines and not storing locally, because VDI is more restrict on use and the flexibility is less.

Microsoft plans are to have 80 % of the internal application in the cloud during next two years and based on this will have 30 % reduction of cost. But in five years from now will be a huge amount of application, storage in the cloud claims Microsoft's CSA. That could be a communication between private and public cloud or hybrid cloud.

7.1.5 Changes in human responsibility, governance and line management when the next generation services are used

The high security performance would indicate on missing some of flexibility but should always be transparence with users. VDI is a part of the solution. The responsibilities and roles for management and employees have high impact on performing security.

7.1.6 Microsoft's efforts in respect to the next generation of awareness campaign

Microsoft is providing a lot of awareness programs for the employees including procedures, information about new products and regulations. Some of the training programs run once per year, some of them twice depending on the category of people going through it. Microsoft for its employees working in sales department would have the awareness based on their working tasks and responsibilities, or for technical staff would have the program more technical oriented and so on. The result of measuring awareness campaign has shown a good impact in performing better security and making users aware of potential risks. Measuring the success of awareness programs has been made by professionals and usually their findings were giving good results.

Microsoft's effort in the future regarding to the awareness campaign is to have much more web based awareness instead of providing awareness training inside the company.

7.1.7 Security of Bring Your Own Device-BYOD

The interviewee gave four main challenges regarding to data in BOYD:

- Where the data are?
- Who owns the data?
- Who secure the data?

- Management solution

Companies should define what kind of applications or services could be used in the device, for instance the usage of any of social networks, in some companies is allowed to use Twitter but not Facebook or vice versa. The procedure of BOYD usage should go through risk assessment and make sure if there is an identity system in this kind of devices if yes then there is possible to have access to some application and data.

7.2 Case Study: ETAVIS GNS AG (Switzerland)

The second case study is hold with a Swiss company called EAVIS GNS AG and its profile is in determining guides through the entire IT maze: Engineering Solutions and Services. The interviewee's task in the company is Senior IT Systems Engineer.

7.2.1 Security officer's tasks using VDI

The interviewee claims that a VDI technology brings the desktop and its data securely, by transmitting the data back in the datacenter in a secure way. Because of that, it is easier to guarantee the security of confidential data itself. The most important part now is the accessibility to virtual desktops and to data from everywhere and with every device. Additionally, users are able to access the company's application from nearly any device. The interviewee claims that the company should be aware of the security importance by implementing policies and also technical systems to provide secure access for selective persons.

7.2.2 Security performance when performed Outsourcing

The interviewee based on his working profile as Senior IT Systems Engineer and based on his experience claims that outsourcing depends on the companies. The company ETAVIS GNS AG is providing its services in collaboration as outsourcing with many costumers including private banks and Small and Medium Business (SMB) costumers. In Switzerland, many companies want so spent money and efforts to build up their own infrastructure and not move to a cloud service by building a private cloud which is more secure comparing with public cloud.

However, for SMB, the public cloud is very interesting and profitable. They can have an enterprise environment, with all redundancy and flexibility without a huge investment. The guess given by the interviewee is that in the future, we will have a lot of SMB in the cloud. Just one stopper is, when they have their own IT Staff and want to keep them.

His beliefs are that in 10 years from now, around 60 % of all companies in Switzerland will work with or complete in a public cloud service.

7.2.3 Impact of security policies in the future

The interviewee is a bit confused regarding of policies impact in the future and with no particular claim of what would come in the future because there are a lot of things going on currently, new products are in the pipeline and the market is now more ready for all this services, like it was two years ago.

In the future many customers will be aware about security policies. IT staff has to move

forward, because the normal (not IT) staff brings its own gadgets and data services. Thus, a company has to bring all IT services needed for daily business, employees without having the need to use Dropbox, because they want to share a file and has just a mail system for that.

7.2.4 The Future market share of new Computing (VDI and cloud services)

The interviewee expect a grow like in server virtualization in the past few years. However, in five years from now, the guess is that 80 % are going to work on VDI or cloud services (hosted in- or outside the company).

7.2.5 Changes in human responsibility, governance and line management when the next generation services are used

It was difficult to claim for anything but an opinion would be that IT Department will be more important for the business and possible subordinated directly beyond the top management.

7.2.6 Your efforts in respect to the next generation of awareness campaign

Working as system engineer for a system integrator is performing the process of consulting the customer about all positive aspects of the new technologies. But also sensitize him about possible risks or new threats. The IT staff has to co-work with the management, so they can build up exactly what the company needs and also have the backing for these projects.

7.2.7 Security of Bring Your Own Device-BYOD

Bring your own device is in every mouth. But it needs time for this new thinking. For some decades the company has provided all the equipment needed for daily work. There must be an effort for the user to use his private device, billing or something like this claimed the interviewee.

BYOD forces the mobility of the users and also gives the ability to work out of business hours The new technologies provide an interface to the business desktop, applications and data. So you have not to manage the users end device. You maintain and provide a secure in house environment and ensure that the access on this is service or device fits to your policy. Also here, it really matters what type of business you are running.

7.3 Case Study: Norsis (Norsk senter for informasjonssikring/ Norwegian Centre for Information Security)

Norwegian Centre for Information Security (NorSIS) is part of the government's commitment for information security in Norway. NorSIS is focused on information security and helps on becoming this area as a part of everyday life by providing:

- Raising awareness against threats and vulnerabilities.
- Providing information and advice for specific measures through training and guidance.
- Establish an overall awareness towards information security.

The target groups are Norwegian companies in private and public sectors. NorSIS professionally works under the ministry of government administration reform and church affairs

7.3.1 Security officer's tasks using VDI

Virtual desktop offers new working opportunities by offering services to the user. This kind of infrastructure indicates on user's focus, where they are not that worried regarding to the security on devices (firewall, ant viruses etc,) where the connection takes place claimed the interviewee. Hence, the more focused area would be in the virtual environment and in the client side, for instance if a particular user is infected and compromised facing with the same problem even the user use another device. This means that clients do not need to be secured twice when using different devices, is just enough by performing security into users profiles and virtualized environment.

To ensure the security when virtual desktop is used the security officer should use technical approaches such as anti viruses, firewall and other programs, but also other methods such as awareness training performing based on the company's profile. Moreover, make strict rules, for instance when employees has finished their work to shut down the computer in order to prevent unauthorized access.

The most important thing for the interviewee is to prevent the clients from being infected, because there are a lot of user's thoughts regarding to virtual desktops security where they do not care that much because of their misunderstanding regarding to what is really important for security performance. Users think that in VDI they they are safe even by clicking into websites with viruses, but this is not true because the virtual machine image of that particular user may be infected in this case.

7.3.2 Security performance when performed Outsourcing

The interviewee thinks that in the future will be more used outsourcing because is cheaper and can is supposed to be more secure but it may happen to be less secure and this mostly would work based on trust.

More cloud services will be used like Dropbox, but using such services has a lot of weaknesses because the entire infrastructure depends on usernames and passwords and this can be a real problem in case of losing the credentials. Hence, taking place this kind of incidents with credentials when outsourcing is used is much more difficult than using internal insource by the company where the problem can be solved by resetting the password or any other procedure. Anyway, companies in the future will use more outsourcing claimed the interviewee.

7.3.3 Impact of security policies in the future

The focus should be more on the human aspects, because usually policies contains instruction how to perform security such as how strong should be the password or another issue but policies should include more procedures and instruction how the hackers works and how they will find the way to perform an attack. In the past years the focus was mainly in technology but recently the IT market started to pay much more attention to the human aspects.

7.3.4 The Future market share of new Computing (VDI and cloud services)

Even the company providing the interview do not sell any product they are using a lot cloud services and based on them in the future the usage of cloud services will be higher and higher.

Infrastructure of the company (NorSIS) is mostly based on the cloud; all the information and data are stored into cloud without using an internal server. Dealing with important data helps the encryption method making the data much more secure. Beside of performing encryption the company may perform other security measures such as defining what kind of devices may be used to access the data.

7.3.5 Changes in human responsibility, governance and line management when the next generation services are used

The management has critical role in performing security and in managing any kind of situation within a company. Changes can be made easier from top management to the bottom. Moreover, when management is involved on educating its employees brings good results, for instance making people aware what kind of information and what generally is allowed to post into social networks sites and also by making users aware that they are responsible for their working and security performance by defining responsibilities for each of them.

7.3.6 NorSIS efforts in respect to the next generation of awareness campaign

NorSIS as a company is providing a lot of awareness programs because they claimed that the user should be educated what is allowed and what is not allowed to do. They are finding new ways or methods to train people by having opportunities to cover big audience. NorSIS as a company in collaboration with some particular institutions is planning to provide awareness program in radio programs where the amount of audience is high and also another idea is to do it on television in some well known programs.

The awareness program would be more interesting and will take more attention to the audience when is performed by humor claimed the interviewees. The humor in awareness program is considered very important for NorSIS. Awareness training should be performed also with little kids by providing them simple information (based on their capacity of thinking) about the potential risks in several circumstances.

7.3.7 Security of Bring Your Own Device-BYOD

Recently most of the companies are allowing employees devices to be used, because they do not want to control people on what kind of devices or operating system to use. Companies are mostly concerned about their security in those devices; anyway they should perform policies and make users aware of what kind of performance is allowed.

Always the encryption of sensitive information is required, but the problem now is the usage of mobile phones where the encryption is rarely performed, even NorSIS do not use encryption into the employees mobile phones, but they perform security measures, for instance receiving an important information by e-mail cannot be opened on their mobile phones but just on the trusted devices.

8 Interviews Discussion

In this chapter is presented a short discussion extracted from interviews analysis. As it was described in chapter 7, the interview questions were sent before the meeting in advance. Shortly the topic description was sent to the participants, and they were supposed to give their opinions and claims in several situations. All the participants were experts in information security; including chief security adviser, senior IT system engineer and senior advisers in information security. The interviews had been realized with the following persons:

1. **Ole Tom Seierstad** [1]**-** Chief Security Adviser at Microsoft of Norway
2. **Angelo Casanova**- Senior IT Systems Engineer at ETAVIS GNS AG (Switzerland)
3. **Vidar Sandland** and **Peggy Sandbekken Heie**-Norsk Senter for Informasjonssikring- NorSIS

8.1 Virtual desktop security

From the first question, we speculate that when Virtual Desktop Infrastructure is used the security is expected to be higher as one of the interviewees claimed "There is much more environmental controls when using virtual desktop", meaning that the entire infrastructure is known for the monitoring staff, including information of what kind of programs are running, what kind of operating systems and some other user's information. In the other hand, VDI is claimed to provide desktop and its data securely by transferring the data into a data center in a secure way and by ensuring the data confidentiality.

Two of the interviewees claimed that to perform security the company should provide technical approaches such as firewall, antiviruses, IDS but great impact would have other methods in educating users or employees such as policies, awareness programs indicating directly on ensuring secure access to the virtual desktop. However, another very important issue when it comes to security performance in virtual desktop is that the main focus should be on the virtual environment and in the client side, and not in the devices.

8.2 Security performance when using Insourcing Outsourcing

In the future more outsourcing services are going to use. Outsourcing is offering advantages like lower cost, working experts on a particular field, easy management of data etc. One of the interviewees claimed that using insourcing and outsourcing by the company should be made through some security measures. Data classification is a key of preventing sensitive data disclosure and confidentiality. Hence, this classification is even more important for companies dealing with important data for themselves and fort its users. This classification should be performed based on business impact of data: high business impact, moderate and low business impact. Dealing with data with high business impact companies usually performs strong security measures such as

[1] http://www.microsoft.com/nb-no/about/ommicrosoft/ledelsen.aspx

data encryption, data accessible based on user's roles and privileges.

Small and Medium Businesses (SMB) usually want to use public cloud because of redundancy and flexibility without investing that much resources into it comparing with private cloud which is more secure but the cost is higher. Using cloud services where username and password are critical if being disclosed making possible unauthorized accessibility and using internal infrastructure makes much easier to solve this problem just by resetting the password, but using external services is much more difficult.

8.3 Security policies impacts

We speculate that security policies would have positive impact even more in the future. Policies as a good indicator in human behavior should contain not only information and guidelines how to behave and act but would be more successful if the user become informed how it works in practice if them as user do not follow policies by giving information how an attacker will approach to user's mistakes by introducing attacks consequences.

When it comes to access confidential and sensitive data the company can provide policies for its users to perform security measures. Policies may define rules in order to access this kind of information, for instance, the user must have the hard drive encrypted otherwise they will have access only into resources with moderate or low business impact.

8.4 Changes in human responsibility, governance and line management

All the interviewees declared that top management in collaboration with IT department within a company would have great impact in dividing roles and responsibilities beyond its employees. To manage any kind of situation top management would be the key of success to handle the incident in proper way. Hence, this would work better also when educating and making users aware of security issues.

8.5 Next generation of awareness campaigns

Awareness campaign will be mostly as it was before by adding continually new systems and technology, educating users how the technology works and how to behave in such circumstances in order to protect information assets. Awareness programs should be supported by top management by finding out the most useful methods depending on the company profile in order to achieve the desired results. Another important issue is to provide awareness based on user's tasks and responsibilities.

To be more interesting and attractive the awareness programs should involve humor approaches and try to cover many people. If the company is providing any kind of services and is having costumers, or if the company is working with information security like NorSIS, in order to educate users of for any kind of technology, other approaches could be included such as radio, TV, newspaper etc.

8.6 Market share of cloud services

All the interviewees gave their opinions on the amount of cloud usage, where the market share is growing every day. In the near future, the cloud and VDI usage will be higher, by moving most

of the companies their infrastructure into cloud.

Organizations with huge market capacity are using cloud but even more is going to be used in five. The idea is that in five to ten years from now 80 % of the applications and organizations infrastructure are going to work on VDI or Cloud. Using cloud services with this capacity will directly indicate into organizations costs in reducing it up to 30 %. Hence, security concerns would be present in the future, and even more when the usage is growing. Companies to protect their information assets, privacy, confidentiality and availability should use strong technology protection systems and providing security measures for users on changing their behavior through policies and awareness programs.

8.7 Security of Bring Your Own Device-BYOD

This new way of working is going to be used even more in the future because most of the companies are allowing it. Companies mostly are concerned about the health of devices using their services or connecting into virtual desktop. Policies, guidelines and awareness campaign would help on improving security performance on their devices, by informing them what is allowed to be used or how to behave when working for the company.

Through BOYD is possible to maintain and provide a secure in house environment and ensure that the access from these devices fits to organizations policies. Policies and procedures when BOYD is used may include the usage of companies' network or the data encryption of all sensitive information.

9 Conclusion and Future Work

Many virtualization platforms are surrounding in today's market, by offering their services to the costumers. The most useful platforms by many companies worldwide are considered to be VMware, Citrix and Microsoft. Features of these three platform has been briefly described in this project, however to find the best one was a bit difficult because most of them are specific and easy manageable but there are also providers that provides services in a bit more complex way. Thus, some vendors are focused more in offering complete sets of functionality, while some of them are focused on providing small solution but with specific functionality. Both of the scenarios are good options, just depends on the costumers functionality needs. Most of virtualization vendors offer the same services providing almost the same features. Nevertheless, a particular virtualization platform may offer a specific service comparing with others as it is shown in the comparison features tables in Appendix B. However, an assessment done by investigating vendor's capabilities and strategies to execute their own chosen strategies has shown that Citrix is in the first place followed by VMware and then other platform including also Microsoft.

Cloud services and VDI usage makes users confused regarding to the technology indications in respect to these new offered approaches. As it is described in the project VDI works by delivering to the user a full access to a standard desktop which runs in virtual machines stored in a centralized data center making possible to be accessed by any device and from any location. Nevertheless, even security measures performs in virtual machines running in a data center, security tools and systems need to be run when accessing into virtual desktop. Purpose of security systems and tools is to provide secure access and prevent the infection of user's virtual machines.

Companies usually are facing with many concerns as presented in subsection 6.5 facing as well as with legal issues where based on them the data are processed and treated, if the company itself is not directly connected on data managing process. This could be one of the reasons that companies hesitate on moving their infrastructure into cloud. However, even cloud providers are dealing with the risk of liability and regulations, reducing the number of services offered by them.

To address security issues and requirements starts by analyzing SLA coverage including the main condition. Hence, this process helps on assessing potential risks by both costumers and providers by including and describing in detail the obligations and rights of business partners included in this process. Such a procedure can involve for the costumer information and notification in regard to security breaches or for the process of data transfer, change of controls and data access. Addressing these issues by SLA would be helpful for both costumers and cloud providers, to get support from law and to make possible the accomplishment of predefined requirements.

Companies using technology systems in protecting information assets in cloud environment usually do mistakes on treating these concerns as technical problems just by adapting systems and tools instead of adapting strategies and regulations based on risk management concepts. However, most of the companies realized that cloud services usage is a need and its time has arrived, but a challenge for them is to update and involve appropriate security strategies and treating more human aspects. Recently, adoption of VDI and cloud service might had impact on the manner that people are living and working with, in terms of the data location, process of transfer and the way that IT systems are integrated. This impact on user's working style depends on the method and the way of provided cloud services. Offered possibilities to access corporate recourses through virtual desktop and cloud services should make employees more responsible and aware about possible threats. Hence, serious threat related to human activities and their negligence could be the ability of looking into the screen when the user attempts to gain access to the company's systems and resources.

Human factor as a critical factor in security performance in cloud environment has grown even more its importance, to make people going through policies and procedures usually it is not impossible to get successfully applied Most of the people do not have the willing to follow policies and procedures, anyway the corporate governance should make rules and find out methods based on its profile making them to follow provided regulations and policies. People are different and they have different attitudes influenced by culture, age, gender, personality, pressure, lifestyle and many other factors and this probably indicates on not having the same influence of the policies to the people. Considering all these indications and security profile within the organization in order to raise the security performance when using virtual desktop and cloud services first is needed to analyze and make risk assessment and based on result taken from this assessment develop security measures.

To perform security controls in respect of treating human aspects in cloud environment, the company should make a step-change in the level of awareness, care and classification of the information and perform security among its staff. However, big challenge is considered to be policies and data security enforcement on a shared infrastructure making cloud policies and awareness much more complex comparing with traditional IT environment. Therefore, policies and awareness program would be a real factor first of all on educating the users by making them aware of their impact in information security and secondly providing information to them how to react and how to handle in case of facing with any possible attack. Anyway, awareness programs should involve understandable information for their users involving humor and making interesting lessons as much as possible. Policy procedures also impacts on human being behavior in providing information on what are allowed to do and what should not do in order to protect company's resources. Security approaches would be more successful if the managers and all the staff realize the importance of virtual desktop, practicing security measures inside the company and beyond its boundaries.

Bibliography

[1] *NIST Special Publication 800-145. 2009. The NIST Definition of Cloud Computing.* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. [Last Visited: March 09th, 2012].

[2] *Rolf Harms and Michael Yamartino. THE ECONOMICS OF THE CLOUD. Microsoft, November 2010.* http://www.microsoft.com/en-us/news/presskits/cloud/docs/the-economics-of-the-cloud.pdf. [Last Visited: May 09th, 2012].

[3] *Lee Yeong Ro. Policy Recommendation and Regional Cooperation. Consultant, ESCAP. November 2010.* http://www.unescap.org/idd/events/2010_EGM-ICT/25-Mr-Lee-ESCAP-recommendaion-draft.pdf. [Last Visited: May 09th, 2012].

[4] Srivastava, A. dec. 2011. vdaas: Reference architecture. In *India Conference (INDICON), 2011 Annual IEEE*, 1 –5.

[5] Mather, T., Kumaraswamy, S., & Latif, S. 2009. *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. O'Reilly Series. O'Reilly.

[6] Cao, C. & Zhan, Z. sept. 2011. Incident management process for the cloud computing environments. In *Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on*, 225 –229.

[7] *FedRAMP Program. Ongoing Assessment and Authorization (Continuous Monitoring).* http://www.fedramp.net/ongoing-assessment-and-authorization-continuous-monitoring. [Last Visited: March 4th, 2012].

[8] Jian-hua, Z. & Nan, Z. aug. 2011. Cloud computing-based data storage and disaster recovery. In *Future Computer Science and Education (ICFCSE), 2011 International Conference on*, 629 –632.

[9] *IBM Global Tehcnology Services. Virtualizing disaster recovery using cloud computing - Transition your applications quickly to a resilient cloud. January 2012.* http://www-935.ibm.com/services/uk/en/it-services/vsr_whitepaper.pdf. [Last Visited: March 4th, 2012].

[10] *Aemon Malone. Amazon experiencing troubles with cloud servers, Reddit and Quora among affected sites. Digital Trends, April 2011.* http://www.digitaltrends.com/computing/amazon-experiencing-troubles-with-cloud-servers-reddit-and-quora-among-affected-sites/. [Last Visited: May 11th, 2012].

[11] Song, I. Idc marketscape: Worldwide desktop virtualization 2011 vendor analysis. Technical report, IDC - Analyze the Future, 2011.

[12] *EnteraSys. Virtual Desktop Infrastructure and the Network: The Data Center becomes the New Edge.* http://www.enterasys.com/company/literature/virtual-desktop-infrastructure-sab.pdf. [Last Visited: June 4th, 2012].

[13] *Kevin Beaver. The real deal with internal security threats. TechTarget.* http://searchwindowsserver.techtarget.com/tip/The-real-deal-with-internal-security-threats. [Last Visited: April 4th, 2012].

[14] Chandran, S. P. & Angepat, M. 2010. Cloud computing: Analysing the risks involved in cloud computing environments. *IRCSE10 Workshop*.

[15] Ramgovind, S., Mm, E., & Smith, E. 2010. The Management of Security in Cloud Computing. *Security*, (March 30 2010-April 1 2010), 1–7.

[16] Sosinsky, B. 2011. *Cloud Computing Bible*. Wiley Publishing, 1st edition.

[17] Zhang, X., Wuwong, N., Li, H., & Zhang, X. 2010. Information Security Risk Management Framework for the Cloud Computing Environments. In *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, 1328–1334.

[18] Kundra, V. 2011. Federal cloud computing strategy. *Position paper of the CIO of the US government*.

[19] Luo, X., Yang, L., Ma, L., Chu, S., & Dai, H. 2011. Virtualization Security Risks and Solutions of Cloud Computing via Divide-Conquer Strategy. In *Multimedia Information Networking and Security (MINES), 2011 Third International Conference on*, 637–641.

[20] *Wikipedia - Qualitative research.* http://en.wikipedia.org/wiki/Qualitative_research. [Last Visited: April 26th, 2012].

[21] Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. 2009. A break in the clouds : Towards a cloud definition. *Computer Communication Review*, 39.

[22] *Dan Farber. September 26th, 2008. Oracle's Ellison nails cloud computing.* http://news.cnet.com/8301-13953_3-10052188-80.html. [Last Visited: May 09th, 2012].

[23] Gong, C., Liu, J., Zhang, Q., Chen, H., & Gong, Z. sept. 2010. The characteristics of cloud computing. In *Parallel Processing Workshops (ICPPW), 2010 39th International Conference on*, 275 –279.

[24] Zhao, G., Rong, C., Jaatun, M. G., & Sandnes, F. E. 2010. Deployment models: Towards eliminating security concerns from cloud computing. In *High Performance Computing and Simulation (HPCS), 2010 International Conference*, 189–195.

[25] Blokdijk, G. & Menken, I. 2009. *Cloud Computing - the Complete Cornerstone Guide to Cloud Computing Best Practices: Concepts, Terms, and Techniques for Successfully Planning, Implementing and Managing Enterprise It Cloud Computing Technology*. Emereo Pty Limited.

[26] *Gartner. Seven Security Risks of Cloud Computing. Gartner, April 2012.* http://www.gartner.com/technology/research.jsp. [Last Visited: April 17th, 2012].

[27] *Jay Heiser and Mark Nicolett. Assessing the Security Risks of Cloud Computing. 3th June 2008*. http://www.gartner.com/id=685308. [Last Visited: April 4th, 2012].

[28] *VMware, Inc. Virtual Desktop Infrastructure: Improved manageability and availability spur move to virtualize desktops.* http://www.vmware.com/pdf/virtual_desktop_infrastructure_wp.pdf. [Last Visited: June 4th, 2012].

[29] *Frank Ohlhorst. Delivering desktop PCs through the cloud. TechTarget.* http://searchvirtualdesktop.techtarget.com/tip/Delivering-desktop-PCs-through-the-cloud. [Last Visited: March 4th, 2012].

[30] *Chhandomay Mandal. Deploying a Storage-optimized Virtual Desktop Infrastructure.*

[31] Velte, T., Velte, A., Velte, T., & Elsenpeter, R. 2009. *Cloud Computing, A Practical Approach*. McGraw-Hill.

[32] Carr, N. 2008. *The Big Switch: Rewiring the World, from Edison to Google*. W.W. Norton and Company.

[33] Buckley, P. 2010. *The Rough Guide to Cloud Computing*. Rough Guides Reference. Rough Guides.

[34] Hugos, M. & Hulitzky, D. 2010. *Business in the Cloud: What Every Business Needs to Know About Cloud Computing*. John Wiley and Sons.

[35] Popovic, K. & Hocenski, Z. may 2010. Cloud computing security issues and challenges. In *MIPRO, 2010 Proceedings of the 33rd International Convention*, 344 –349.

[36] Jansen, W. jan. 2011. Cloud hooks: Security and privacy issues in cloud computing. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, 1 –10.

[37] *Wayne Jansen and Timothy Grance. Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-114. December 2011.* http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf. [Last Visited: March 09th, 2012].

[38] Krutz, R. & Vines, R. 2010. *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. John Wiley & Sons.

[39] Wood, T., Cecchet, E., Ramakrishnan, K. K., Shenoy, P., van der Merwe, J., & Venkataramani, A. 2010. Disaster recovery as a cloud service: Economic benefits & deployment challenges. In *Proceedings of the 2nd USENIX conference on Hot topics in cloud computing*, HotCloud'10, 8–8, Berkeley, CA, USA. USENIX Association.

[40] Rittinghouse, J. & Ransome, J. 2009. *Cloud Computing: Implementation, Management, and Security*. CRC Press.

[41] *SNIA (Storage Networking Industry Association). Managing Cloud Backups.* http://www.snia.org/. [Last Visited: April 11th, 2012].

[42] *Cloud Security Alliance (CSA). Manage Cloud Redundancy. September 2011.* https://blog.cloudsecurityalliance.org/2011/09/. [Last Visited: May 11th, 2012].

[43] *Steve Shah. Citrix, Microsoft and VMware: Comparing virtualization strategies. TechTarget.* http://searchvirtualdesktop.techtarget.com/tip/Delivering-desktop-PCs-through-the-cloud. [Last Visited: March 4th, 2012].

[44] *Christine Taylor. EMC and Private Cloud/VMware Security. April 4th, 2012.* http://tanejagroup.com/news/blog/cloud/emc-and-private-cloud-vmware-security. [Last Visited: May 27th, 2012].

[45] *Microsoft Corporate. Microsoft VDI Suite Benefits.* http://www.microsoft.com. [LastVisited:May27th,2012].

[46] Wilson, P. August 2011. Positive perspectives on cloud security. *Inf. Secur. Tech. Rep.*, 16(3-4), 97–101.

[47] Lacey, D. 2009. *Managing the Human Factor in Information Security: How to Win Over Staff and Influence Business Managers*. John Wiley & Sons.

[48] *Computer and Communications Industry Association (CCIA). Public Policy for the Cloud: How Policymakers Can Enable Cloud Computing. July 2011.* http://www.ccianet.org/CCIA/files/ccLibraryFiles/Filename/000000000528/CCIA-PublicPolicyfortheCloud.pdf. [LastVisited:May27th,2012].

[49] *Daniele Catteddu and Giles Hogben. Cloud Computing: BENEFITS , RISKS AND RECOMMENDATIONS FOR INFORMATION SECURITY. ENISA, 2009.* http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/.[LastVisited:May27th,2012].

[50] Kurta, M. On the road towards cloud computing services. Master's thesis, Erasmus School of Economics, 2010.

[51] Teneyuca, D. 2011. Internet cloud security: The illusion of inclusion. *Information Security Technical Report*, 16(3–4), 102 – 107. <ce:title>Cloud Security</ce:title>.

[52] Takabi, H., Joshi, J., & Ahn, G. nov.-dec. 2010. Security and privacy challenges in cloud computing environments. *Security Privacy, IEEE*, 8(6), 24 –31.

[53] Massonet, P., Naqvi, S., Ponsard, C., Latanicki, J., Rochwerger, B., & Villari, M. may 2011. A monitoring and audit logging architecture for data location compliance in federated cloud infrastructures. In *Parallel and Distributed Processing Workshops and Phd Forum (IPDPSW), 2011 IEEE International Symposium on*, 1510 –1517.

[54] *Michael Brandenburg. Bringing BYOD to Your Enterprise. TechTarget.* http://searchmobilecomputing.techtarget.com/tutorial/Bringing-BYOD-to-your-enterprise. [Last Visited: April 4th, 2012].

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

[56] *Wikipedia - Microsoft Application Virtualization (App-V).* http://en.wikipedia.org/wiki/Microsoft_App-V. [Last Visited: May 26th, 2012].

[57] *Wikipedia - SkyDrive.* http://en.wikipedia.org/wiki/SkyDrive. [Last Visited: May 26th, 2012].

[58] *Wikipedia - Microsoft SharePoint.* http://en.wikipedia.org/wiki/Microsoft_SharePoint. [Last Visited: May 26th, 2012].

APPENDIXES

A Interview Questions used for Case Studies

A.1 Main Questions

1. How does the task of the security officer change when virtual desktop is applied?
2. What is your opinion about sharing information, what is Insource and outsource in companies in 5 or 10 years from now (in the future)?
3. Which changes do you expect for good security policies in the future (in context of cloud services and VDI)?
4. What the change is in human responsibility, governance and line management when the next generation?s services are used (VDI, extensive cloud usage, BYOD)?
5. What would be the Microsoft?s efforts in respect to the next generation of awareness campaign?
6. What is your opinion about the market share of the new computing (VDI and cloud services today and in 5 years from now)?
7. BYOD: Do you see any need that companies still are providing company devices, or they completely change the world that everybody has its own device and when we look in the future - 5 to 10 years from now what could be scenario or what it means for information security strategies and what would be the potential market of BYOD?

A.2 Sub Questions

- What are the technical and organizational measures that the company should take to implement the VDI?
- The security level in devices running any virtualization platform is important, but what is the minimum security level in the device where the access into VDI is happening?
- Based on your experience, did you face with security incidents such as data leakage, credentials theft or any other security event?
- Usually, from what was the incident caused, for instance by system failure, infrastructure or by human failure?
- For instance people working in a task may have the whole information of particular costumers or organization information so, who is the owner of database, I mean how you think that employee will cheat a game with customers? data?
- Who is responsible for encryption of data; the virtualization vendors (i.e. Microsoft, Citrix, VMware) or users?
- Who is the owner of the encrypted data and who has access into these?

- Is there any difference when an employee works outside the company, what security measures are provided in this case?
- How the security picture moves when employees go beyond the company borders?
- Do you make aware users through awareness training or by providing policies regarding to the security risk?
- What is usually includes and treats in a security awareness program?
- Do you provide specific policies for the users how to behave when VDI is used?
- In what Companies are focused more in technological issues or human aspects?
- How important are human aspects for you, regarding to VDI security?
- In what level are treated human aspects in VDI environment?
- What do you usually include and treat in a security awareness program?
- Do you think that awareness training make good impact on employees and respect them?
- As a CISO, in what you are focused more in technological issues or human aspects?
- What is important for BYOD: Usability or security?
- Who benefits more from BYOD: the company or employees?
- What you believe is the potential market of BYOD, today and 5 years from now and in which way Microsoft is supporting this?

B Comparison of Virtualization Vendors' Features

Table 3: General comparison of vendors' features.

General		vmware	Microsoft	CITRIX
Version		vSphere 5	Hyper-V R2 sP1	XenServer 6
Edition		Enterprise Plus	DataCenter	Platinum Edition
Assessment	Market Position	Leader (P1)	Leader (P2/3)	Leader (P2/3)
Pricing	Virtualization ($)	Ent+: $3,495/socket/enables 96GB vRAM (NEW!) + S&S: $734 (B) or $874 (Prod), vSphere Desktop: $65/active desktop New	DataCenter: $2,999/socket	$5000/server+ $3000 (support)
	Management ($)	$4,995(S) + $1,049 (B) or $1,249 (P), $1,495(Fnd) + $545(B) or $645(P)	SMSE: $1569/host) or SMSD: $1310 SMSD/CPU (2 CPU min)	Free (XenCenter)
	Guest OS Licensing	Not included	yes - unlimited (Windows)	No

Table 4: Comparison of management module between virtualization vendors.

Management		vmware	Microsoft	CITRIX
Version		vSphere 5	Hyper-V R2 sP1	XenServer 6
Edition		Enterprise Plus	DataCenter	Platinum Edition
General	Central Management	Yes (vCenter Server + vCenter appliance - NEW)	Yes (SCVMM/SMSE/ SMSD)	Yes (XenCenter), SCVMM (new)
	Virtual and physical	No	Yes	Limited
VM Mobility	Live Migration of VMs	Yes vMotion and Metro vMotion	Yes Live Migration (1)	Yes XenMotion (1)
	Automated Live Migration	Yes (DRS) - Storage (NEW), CPU, Mem,	Semi-Integr.(CPU,Mem, 3rd party)	Yes (WB) - CPU, Mem, D, N
	Power Management	Yes (DPM)	Limited	Yes
	Storage Migration	Yes (Storage vMotion / DRS-automated - NEW)	Limited (Partially Live)	No (offline only)
HA/DR	Integrated HA (Restart vm)	Yes (VMware HA) - incl Storage heartbeat	Yes	Yes
	VM Lockstep Protection	Yes (Fault Tolerance)	No	No
Updates and Backup	Hypervisor Upgrades	Yes (Update Manager) - enhanced	Yes	Limited (rolling upgrade wizard - new)
	Integrated Backup	Yes (Data Recovery)	Yes (WSB&DPM)	Yes (VMPR)
Other	Security	Yes (ESXi Firewall - NEW) and (vShield Zones)	Yes	Yes

Table 5: Comparison of Hypervisor between virtualization vendors.

Hypervisor		vmware	Microsoft	CITRIX
Version		vSphere 5	Hyper-V R2 sP1	XenServer 6
Edition		Enterprise Plus	DataCenter	Platinum Edition
Host Config	Max Consolidation Ratio	512vm, 2048 vcpu	384 vm, 8/12 vCPU per core,	75 (up to 130 - see details)
	Max CPU - Host	160 (Logical)	64 (Sockets) 64(Logical)	64 (logical)
VM Mobility	Max Cores per CPU	unlimited	unlimited	unlimited
	Max Memory - Host	2TB	1TB	1TB
VM Config	Max vCPU per VM	32	4(Win) / 4(Linux)	16 (Win) / 32(Linux)
	Max RAM per VM	1TB	64GB	128GB
Storage	Storage Integration (API)	Yes (VASA - NEW, VAAI and VAMP)	Windows Ecosystem	Integrated StorageLink
	Storage QoS	Yes (SIOC) - incl. NFS - NEW	No	Basic
Networking	Distributed Network Switch	Yes (vDS), NetFlow + Port Mirror + LLDP - NEW	No	Yes (Fail-Save Mode - new)
	Network QOS	Yes (NetIOC), custom Resource Pools + IEEE 802.1p - NEW	No	Yes
Memory	Dynamic / Over-Commit	Yes (Memory Ballooning)	Yes (Dynamic Memory)	Yes
Interoperability	Scripting / APIs	CIM / SMASH API, SDKs for web services, Perl, Power CLI etc	Yes (PowerShell, WMI API)	Yes (SDK, API, PowerShell)
Hot add support		CPU, memory, disk, NIC	Disk	Disk, NIC

Table 6: Comparison of cloud services between virtualization vendors.

Cloud (draft)		vmware	Microsoft	CITRIX
Version		vSphere 5	Hyper-V R2 sP1	XenServer 6
Edition		Enterprise Plus	DataCenter	Platinum Edition
Comment	Draft (VMware only)	General Vendor capabilities - not edition specific (typically vCloud functionality is only supported with Enterprise editions).	TBA	TBA
IaaS (Private)	Product Name	vCloud Director (vCD)	TBA	TBA
Hybrid	Hybrid 'Connector'?	vCloud Connector	TBA	TBA
IaaS (Public)	What? Offering Name	1) vCloud Express (test/dev, public, PAYG) 2) vCloud DataCenter Services (Enterprise, Hybrid, PAYG to dedicated)	TBA	TBA
PaaS	Offering Name	CloudFoundry	TBA	TBA
SaaS	Product name(s)	Limited - Zimbra, Horizon App Mgr	TBA	TBA

Table 7: Comparison of Business Continuity between virtualization vendors.

Business Continuity	vmware	Microsoft	CITRIX
Version	vSphere 5	Hyper-V R2 sP1	XenServer 6
Edition	Enterprise Plus	DataCenter	Platinum Edition
High Availability	Yes	Yes	Yes
Restart prioritization	Yes	Not included	Yes
Fault tolerance (zero downtime HA)	Yes	Not included	Yes
Disaster/site recovery	Yes *3 (SRM)	Yes (MSCS)	Yes
Live migration	Yes	Yes	Yes
Long distance live migration	Yes	Not included	Not included
Hosts per cluster	32	16	16
VM's per host	512	384	75
VM's per cluster	300	1000	800

Table 8: Comparison of Guest (VM) Operating System Support between virtualization vendors.

Guest (VM) Operating System Support	vmware	Microsoft	CITRIX
Version	vSphere 5	Hyper-V R2 sP1	XenServer 6
Edition	Enterprise Plus	DataCenter	Platinum Edition
Microsoft Windows 8 32-bit	No	No	No
Microsoft Windows 8 64-bit	No	No	No
Microsoft Windows 7 32-bit	Yes	Yes	Yes
Microsoft Windows 7 64-bit	Yes	Yes	Yes
Microsoft Windows 7 SPI	Yes	Yes	Yes
Microsoft Windows Vista 32-bit	Yes	Yes	Yes
Microsoft windows Vista 64-bit	Yes	Yes	Yes
Microsoft Windows XP	Yes	Yes	Yes
MS Windows 95/98	No	No	No
MAC OS X	No	No	No
Linux CentOS	No	No	No

Table 9: Comparison of Client (Endpoint) System Operating Support between virtualization vendors.

Client (Endpoint) Operating System Support	vmware	Microsoft	CITRIX
Version	vSphere 5	Hyper-V R2 sP1	XenServer 6
Edition	Enterprise Plus	DataCenter	Platinum Edition
Microsoft Windows 8 32-bit	No	No	No
Microsoft Windows 8 64-bit	No	No	No
Microsoft Windows 7 Professional	Yes	Yes	Yes
Microsoft Windows Vista Professional	Yes	Yes	Yes
Microsoft Windows XP Professional	Yes	Yes	Yes
Microsoft Windows 2000 Professional	No	No	No
Microsoft windows Server 2003R2	Yes	Yes	Yes
Microsoft Windows Server 2008	Yes	Yes	Yes
Microsoft Windows Server 2008 R2	Yes	Yes	Yes
Windows 9X	No	No	No
Windows XPe	Yes	Yes	Yes
Windows CE	Yes	No	Yes
Windows Embedded Standard 7	Yes	Yes	Yes
MAC OS X	Yes	Yes	Yes
Any OS running Java	No	No	Yes
Unix flavors	No	No	Yes
Linux flavors	Yes	No	Yes
Linux- Ubuntu	Yes	No	Yes
Apple iPhone/iPod v4.x	No	No	Yes
Windows Phone 7	No	No	No

Table 10: Comparison of Internet Browser support for web based access to virtual desktop between virtualization vendors.

Internet Browser support for web based access to virtual desktop	vmware	Microsoft	CITRIX
Version	vSphere 5	Hyper-V R2 sP1	XenServer 6
Edition	Enterprise Plus	DataCenter	Platinum Edition
Internet Explorer 6.x	Yes	Yes	Yes
Internet Explorer 7.x	Yes	Yes	Yes
Internet Explorer 8.x	Yes	Yes	Yes
Internet Explorer 9.x	Yes	Yes	Yes
Mozilla Firefox 2.x	Yes	No	Yes
Mozilla Firefox 3.x	Yes	No	Yes
Opera v9	Yes	No	Yes
Safari v4	Yes	No	Yes
Safari v5	Yes	No	Yes
Google Chrome	Yes	No	Yes
Java Client	Yes	No	Yes