

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

FACULTY OF ECONOMICS AND MANAGEMENT



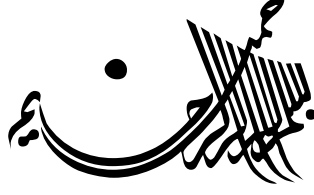
Cloud computing technology framework and reducing risks

Dissertation thesis

Author: Ing. Khaled Ali Ahmed Akrir

Advisor: doc. Ing. Zdeněk Havlíček, CSc.

Department of information technology



(قُلْ إِن صَلَاتِي وَنُسُكِي وَمَحْيَايَ وَمَمَاتِي لِلَّهِ رَبِّ الْعَالَمِينَ (162) لَا شَرِيكَ لَهُ وَبِذَلِكَ أُمِرْتُ وَأَنَا أَوَّلُ الْمُسْلِمِينَ)

صَدَقَ اللَّهُ الْعَلِيمُ

Declaration

I declare that I have worked on my diploma thesis titled “Cloud computing technology framework and reducing risks” by myself and I have used only the sources mentioned at the end of the thesis.

In Prague on 19th of May, 2015

Ing.Khaled Ali Ahmed Akrir

Acknowledgements

I want to give my wholehearted appreciation and deepest gratitude for the assistance and relentless guidance provided by doc. Ing. Zdeněk Havlíček, CSc. in his supervision of my research efforts. Doc. Ing. Zdeněk Havlíček, CSc. Worked tirelessly, without his guidance, this research would not have been possible. He convinced me to stop boiling the ocean and focus on the key research aspects necessary to accomplish the dissertation. I also want to thank Ing. Miloš Ulman, Ph.D. for his helping, by reviewing my research approach and providing many brilliant ideas on how to achieve successful qualitative research. I also want to thank all the technical experts within HP, ORACLE CLOUD, and IBM Czech republic, and the many companies that participated in the interview process and that donated generously to this research through security information and statistical data. I also want to thank the IT management department, team members at CZU for the fabulous support they provided, and for the way they became part of my extended family as a result. I want to acknowledge my family, for their support, I will always love them.

Abstract

The thesis investigates, in a qualitative way, the vectors that contribute to cloud computing risks in the areas of security, business, and compliance. The focus of this research is on the identification of risk vectors that affect cloud computing and the creation of a framework that can help IT managers in their cloud adoption process. Economic pressures on businesses are creating a demand for an alternative delivery of the model that can provide flexible payments, dramatic cuts in capital investment, and reductions in operational cost. Cloud computing is positioned to take advantage of these economic pressures with low cost IT services and a flexible payment model, but at what risk to the business? Security concerns about cloud computing are heightened and fueled by misconceptions related to security and compliance risks. Unfortunately, these security concerns are seldom, expressed quantifiably. To bring clarity to cloud computing security, compliance, and business risks, this research focuses on a qualitative analysis of risk vectors drawn from one-on-one interviews with top IT experts selected. The qualitative aspect of this research separates facts from unfounded suspicions, and creates a framework that can help align perceived risks of cloud computing with actual risks. The qualitative research was done through interviews with experts and through the survey to measure risk perceptions about cloud computing using a Likert scale. The decision-making model and the framework created by this research help to rationalize the risk vectors on cloud environments and recommend reducing strategies to bring the IT industry one step closer to a clearer understanding of the risks-tradeoffs implications of cloud computing environments.

Keywords

Cloud computing, CSRF, CBRF, CCRF, Cloud Provider ,Cloud assets, Compliance, Expert, IT Professional ,Threat ,Vulnerability, Attack, Risk.

Abstrakt

Práce zkoumá kvalitativním způsobem vektory, které přispívají k rizikům cloud computingu v oblasti bezpečnostní, obchodní a shody standardů. Zaměření tohoto výzkumu je na identifikaci rizikových vektorů, které mají vliv na cloud computing a vytvoření rámce, který může pomoci IT manažerům v procesu přijetí cloudu. Ekonomické tlaky na podniky vytvářejí poptávku po alternativních dodávkách pomocí modelu, který může poskytnout flexibilní platby, dramatické škrty v oblasti kapitálových investic a snížení provozních nákladů. Cloud computing je schopen využít těchto ekonomických tlaků na poskytování nízkonákladových IT služeb a flexibilního platebního modelu, ale s jakým rizikem pro podnikání? Bezpečnostní obavy cloud computingu jsou zvýšeny a podporovány mylnými představami o zabezpečení a riziky spojenými s dodržováním předpisů. Bohužel, tyto obavy o bezpečnost jsou zřídka vyjádřeny kvantifikovatelně. Cílem je vyjasnit cloud computing zabezpečení, dodržování předpisů, a podnikatelská rizika, proto se tento výzkum zaměřuje na kvalitativní analýzy rizikových vektorů čerpané z individuálních rozhovorů se špičkovými IT odborníky ve vybraných společnostech. Kvalitativní aspekt tohoto výzkumu odděluje fakta od nepodložených podezření a vytváří rámec, který může pomoci sladit vnímaná rizika cloud computingu s aktuálními riziky. Kvalitativní výzkum byl proveden prostřednictvím rozhovorů s experty a prostřednictvím průzkumu vnímání rizik ohledně cloud computingu pomocí otázek a odpovědí s využitím Likertovy stupnice. Rozhodovací model a rámec pomáhají racionalizovat rizikové vektory v cloudovém prostředí a doporučit strategie ke snížení rizik tak, aby IT průmysl byl o krok blíže k jasnějšímu pochopení rizik a kompromisů, které vyplývají z důsledků prostředí cloud computingu.

Klíčová slova

Cloud computing, CSRF, CBRF, CCRF, poskytovatel cloudu, cloud aktiva, shoda, expert, IT profesionál, hrozba, zranitelnost, útok, riziko.

Contents

1. Introduction.....	1
1.1 Problem statement	2
1.2 Goal of thesis	4
1.3 Research questions	6
1.4 Research approach	9
2. Literature Review.....	12
2.1 Cloud computing	12
2.2 Hypervisor	21
2.3 Cloud elasticity	22
2.4 Cloud reliability	23
2.5 Cloud APIs vulnerabilities.....	26
2.6 Hypervisor vulnerabilities	27
2.7 Cross-VM Information leakage	35
2.8 Mobile madness	38
2.9 Human Factors - the security weakest link.....	41
2.10 Compliance and regulations	44
2.11 Other efforts engaged in cyber security.....	47
3. Research materials and methods.....	49
3.1 Qualitative method	49
3.2 Delphi research process	53
3.3 Calibration process	58
3.4 Survey.....	59
4. Research outcomes (risks resources of cloud technology)	78
4.1 Highlighting.....	78
4.2 Explanation of main cloud risks.	79
4.3 Framework risks of cloud computing.....	86
4.4 Cloud risks pyramid bases on experts	87
5. Discussion and interviews result.....	89
5.1 Cloud security risks framework (CSRF)	89
5.2 Cloud business risks framework (CBRF).....	104

5.3	Cloud compliance risks framework (CCRF)	116
6.	Survey results and recommendations.....	123
6.1	Survey results	123
6.2	Recommendations for cloud computing adoption.....	130
6.3	Other outcomes.....	131
6.4	Workloads for clouds.....	131
6.5	Some warnings when handling cloud images.....	133
6.6	Future and early work on cloud computing.....	133
7.	Conclusion	135
8.	References.....	140
9.	Appendix A.....	147
10.	Appendix B	153
11.	Appendix C	154

List of Table

Figure 1 Visual Comparison between Traditional IT Risks and Cloud Computing Risks 9

Figure 2 typical delphi method 11

Figure 3 Wavelength Price Declines on Major Routes, Q4 2011–Q4 2012..... 13

Figure 4 change in time GC vs. CC 17

Figure 5 migration man-in-the-middle attack performed by John Oberheide .. 26

Figure 6 Virtualization vulnerability severity by year reported, 1999-2009 28

Figure 7 Critical severity vulnerabilities by year (CVSS = 10 29

Figure 8 Cloud virtualization components..... 30

Figure 9 KVM Architecture..... 32

Figure 10 Xen Architecture. 32

Figure 11 Hypervisor vulnerabilities by Hypervisor and Vulnerability types . 33

Figure 12 Vulnerabilities by Cloud Virtualization Components 1999-2009.... 35

Figure 13 the worldwide mobile phone market 39

Figure 14 Total Mobile Operating System Vulnerabilities 40

Figure 15 Channels between control and business processes 46

Figure 16 Steps followed by qualitative research 50

Figure 17 the modified Delphi 57

Figure 18 Cloud Risks Based on Experts 88

Figure 19 Benefits of Cloud Investment 105

Figure 20 Cloud Server Comparison 114

Figure 21 Alternative Schema 118

Figure 22 Cloud Security and Compliance Risks Model 137

Figure 23 Cloud Business Risks Model..... 138

Figure 24 Results on business risks framework calibration 154

Figure 25 Results on security risks framework calibration 155

Figure 26 Results on compliance risks framework calibration..... 156

List of figures

Figure 1 Visual Comparison between Traditional IT Risks and Cloud Computing Risks	9
Figure 2 typical delphi method	11
Figure 3 Wavelength Price Declines on Major Routes, Q4 2011–Q4 2012.....	13
Figure 4 change in time GC vs. CC	17
Figure 5 migration man-in-the-middle attack performed by John Oberheide ..	26
Figure 6 Virtualization vulnerability severity by year reported, 1999-2009	28
Figure 7 Critical severity vulnerabilities by year (CVSS = 10	29
Figure 8 Cloud virtualization components.....	30
Figure 9 KVM Architecture.....	32
Figure 10 Xen Architecture.	32
Figure 11 Hypervisor vulnerabilities by Hypervisor and Vulnerability types .	33
Figure 12 Vulnerabilities by Cloud Virtualization Components 1999-2009....	35
Figure 13 the worldwide mobile phone market	39
Figure 14 Total Mobile Operating System Vulnerabilities	40
Figure 15 Channels between control and business processes.....	46
Figure 16 Steps followed by qualitative research	50
Figure 17 the modified Delphi	57
Figure 18 Cloud Risks Based on Experts	88
Figure 19 Benefits of Cloud Investment.....	105
Figure 20 Cloud Server Comparison	114
Figure 21 Alternative Schema	118
Figure 22 Cloud Security and Compliance Risks Model	137
Figure 23 Cloud Business Risks Model.....	138
Figure 24 Results on business risks framework calibration	154
Figure 25 Results on security risks framework calibration	155
Figure 26 Results on compliance risks framework calibration.....	156

1. Introduction

The thesis presents an analysis of cloud computing risks associated with security, compliance and business risks. The research focuses on helping IT managers in their ongoing risk trade-off efforts, which must always balance the demands of the business, constant regulatory changes that must be met and escalating security threats (1). IT managers and CIOs engage in a relentless battle to maintain the confidentiality of dealings and the protection of information, and they spend a lot of money to make sure delicate data is kept protected. Nevertheless, IT security problems accounted for more than 160 major security breaches from January 2010 to April 2011 (2). When the cloud computing becomes more persistent, many organizations are considering moving mission-critical workloads to cloud processing environments. However, doubt and limitations to adopting continue to persist due to issues about security, conformity, and business threats, as well as the lack of an efficient design to justify and evaluate IT threats in cloud processing services.

The research concentrates on a qualitative research of Cloud Computing & IT threats that are motivated by security, conformity, and business issues, and efforts to provide a design to justify these threats. In addition, a structural framework is provided to assist in the assessment and execution of Cloud computing, with minimization techniques to decrease IT threats.

1.1 Problem statement

Cloud computing technologies change our world; we are using many of these services without even being aware we are doing it. Every time we do a Google search, post a comment on our social networking site (Facebook, twitter, etc.) or use our cell phone internet, we are using a cloud. The ubiquity of cloud computing on the retail side of information technology seen with the rapid growth of cloud-enabled smartphones, which experienced 27.2 percent growth by 918.6 million smartphones ship to the market in 2013 than 722.4 million units shipped in 2012 (3). Other aspects, such as the commoditization of hypervisor technology and the increase of new operating system (OS) and middleware for cloud computing, have created new security areas for strikes. Large storage space, designed for the pressing need to gather an ever-increasing amount of data, are producing new difficulties in the area of regulating compliance. Finally yet importantly, financial pressures on IT organizations to produce more services with lower budgets are creating significant demands for the adoption of alternative models that could potentially lower the cost of IT. Corporations are attracted to cloud services because of the potentially lower cost of compute services, no capital investment, and flexible payment schedule. However, cloud computing has standardization requirements and a philosophy of “one size fits all” that sometimes does not fit the needs of large corporations. However, the areas that are causing the most concern among IT professionals attempting to use cloud services for mission critical workload are security, technology immaturity, and business issues. These issues include good cost estimates, interoperability and integration with other “not-cloud” services, as well as issues related to downtime and reliability. The 2010 IDC survey highlighted these concerns, with approximately 70 percent of the surveyed population expressing security concerns about cloud environments (4). This research performs a qualitative analysis about key cloud computing IT risks to assist in the creation of a model that can help explain the current security, compliance and business risks associated with cloud computing. This research also attempts to help differentiate between perceived risks and actual risks associated with cloud services.

Through this research we will refer to cloud computing or cloud as the concept of a public compute utility connected to the Internet, where resources are virtualized and shared across multiple tenants, and accessible on demand through an easy-to-use portal or command line. However, it is important to acknowledge, that there are other cloud computing, offerings, such private clouds that have different characteristics, and other architecture derivatives, that contain different configurations.

These variants of cloud computing will be discussed in Chapter 2 as part of the literature review. In addition, the word “risk” is use within the context of this research to refer to the aggregate risk of security, compliance, and business risks that corporations might experience using cloud services.

1.1.1 Key definitions:

Cloud computing – Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models (5)

CSRF- cloud security risks frameworks

CBRF- cloud business risks frameworks

CCRF- Cloud compliance risks frameworks

Cloud Provider – Refers to a supplier of cloud infrastructure as a service (IaaS) that sells the service on a utility computing basis. Examples of cloud providers are Amazon, Rackspace, and IBM.

Cloud assets – Collection of system resources and data on file systems and databases.

Compliance – Law or government regulation that imposes a process required to do business. Examples of compliance regulations include the Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act

(HIPAA), the Sarbanes-Oxley Act (SOX), the Statement on Auditing Standards No. 70 (SAS 70), and the Payment Card Industry (PCI) specifications.

Expert- has done at least one cloud or security implementation.

IT Professional – has using deal with information security

Threat – Potential occurrence of an event that can harm the cloud assets, prevent compliance or inhibit business activities. The event can have a benign basis, such as an unintentional mistake, or it can be from a malicious source.

Vulnerability – Weakness that makes a threat possible

Attack – An action taken to realize threats or abuse vulnerabilities.

Risk – The possibility of loss. This includes the chances of an attack, negative impact to the business, or compliance failure.

1.2 Goal of thesis

The aim of the thesis is to bring clarity and to create a better understanding of the security, business, and compliance risks associated with cloud computing, and to align perceived risks with actual risks. There is much discussion about cloud computing in magazines and blogs across the Internet, but there are very few reliable sources, that document the facts about cloud risks and adoption principles to reduce possible risks. We are in the early stages of cloud computing adoption and cloud providers are competing with each other to establish their offerings. Lack of well-documented cloud standards and cloud certifications are hindering the ability to classify clouds using appropriate measurements or characteristics. IT vendors continue to rely on quality of service (QoS) characteristics to evaluate clouds without appropriate acknowledgment of more important risk factors that plague cloud services.

This analysis research will try to builds a model from the knowledge and insight gathered from interviews with more than sixty cloud and security industry experts and users.

The main goal of this research is to create a model that can guide IT professionals in the understanding of security, compliance, and business risks associated with cloud offerings, and tradeoffs that could reduce these risks.

A model that can help categorize and value cloud-computing risks is a significant contribution to the IT community, and computing science body of knowledge,

These are some of contributions for the IT community, which this research delivers.

1. Provides guidance to rationalize risks associated with cloud computing environments in a way to foster better understanding of cloud services.
2. Provides analogies with common situations and other industries to put into perspective the risks associated with cloud offerings. Unfortunately, news media have exaggerated the levels of perceived cloud risk based on isolated incidents that are very unlikely to affect most users. The net effect is the distortion of perceived risk about cloud environments held by many IT professionals. This research will try to provide a model to evaluate risks and help align perceived risk with actual risk.
3. Provides guidance to minimize the overestimation of cloud capabilities, including elasticity, availability, and performance. In addition, helps estimate the challenges associated with moving workloads to the cloud to obtain horizontal scaling (elasticity) and other cloud features.
4. Creates three cloud frameworks for the evaluation and understanding of security, business, and compliance risks.
5. Identifies risks vectors affecting each of the cloud frameworks and provides reducing strategies to minimize possible exposures to ensure selected workloads perform as expected and at a good price point.
6. explains the value of cloud computing, which workloads are best to move to the cloud to take advantage of low-cost IT.
7. Identifies the cloud risk perceptions of IT professionals, based on the results of a survey targeted to IT cloud professionals.

1.3 Research questions

The main purpose of this research is to analyze the security, compliance, and business risks associated, with cloud implementations, and to help align an individual's perceived risks with the actual risks. This qualitative research leverages the power of Online Questions form and interviews to collect the insights of number cloud and security experts regarding risk associated with cloud computing. The interviews followed a flexible format to allow the free exchange of information and constructive interaction. The interview process was customized to fit the expertise of the individuals interviewed and to collect data and insight on the research questions. The fundamental questions this research is focus on included:

- What new technologies are associated with cloud computing?
- What new values do clouds provide?
- Are there any new security, compliance, and business risks associated with cloud computing?
- Are there any gaps or misalignment between actual cloud computing risks uncovered through interviews with experts and IT professionals' perceived risks?

The questions listed on Table 1 will be used during the interview and online form process with subject matter experts to collect facts about cloud computing risks, and to document the current actual risks associated with clouds. This research also creates a framework to reduce risks associated with cloud services and to help IT professionals benefit from cloud computing.

Table 1: Research Questions

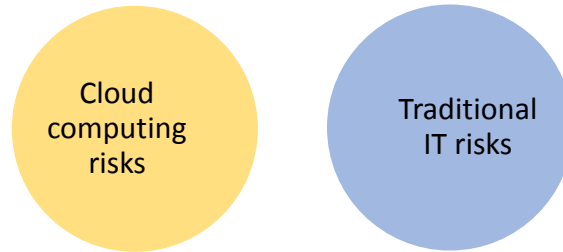
No.	Research Questions
1	Are there any new security, business, and compliance risks associated with cloud computing technologies and services?
2	How do cloud computing technologies and services increase, decrease, or perhaps don't affect security, business and compliance risks?
3	What cloud computing characteristics are generating the most positive and negative impacts on security, business, and compliance risks?
4	What is the best way to detect and protect a cloud against vulnerabilities and malicious attacks? Do you have any risk reducing recommendations?
5	Can cloud computing frameworks and industry certificates help evaluate and reduce security, business, and compliance risks?
6	What applications or solutions are appropriate to run on clouds?

These concerns were motivated by the Gartner study 2011 (6) analytical about the protection issues when applying to cloud computing. This investigation examines many of the cloud issues outlined by the Gartner survey (6) round protection weak points, information selection, comfort problems, as well and insufficient Local Security Regulators (LSAs). The Gartner (6) exposed that dissimilar cloud promotions have actual different stages of protection and that conventional audits like the Declaration on Review Standards No. 70 (SAS70) are not an impermeable of security or governing compliance. The Gartner survey left many demands unreciprocated concerning the value of inspecting cloud services, and how to evaluate cloud risks. Also offered no clarification for the threat vectors affecting cloud services. The Gartner research offered understanding on current cloud problems but left cloud customers with no base for how to assess or assess the threats associated with a cloud offering. This research goes further into the actual problems and clarification of cloud risk vectors and distinguishes information from misguided or unreasonable fears. This research conducted a qualitative research through Online Questions form and interviews with

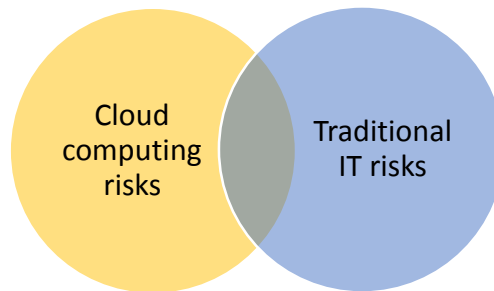
cloud and security experts, and examined the resource of cloud threats evaluate to conventional IT. This research will to find a structure to help IT supervisors in rationalizing security, business and compliance risks. Moreover, this analysis will try provides minimization techniques for each of the threats recognized by the professionals during the On the Online Questions type and interviews. In addition, the qualitative plan of this examination followed a natural viewpoint of the threats related to cloud computing. More specifically, the research collected adequate proof, based on discussions with topic experts, to help recognize an precise visible presentation of the current state of cloud computing threats compared to conventional IT understanding of the existing state of cloud computing risks matched to traditional IT. By traditional IT, we mention to IT facilities that are introduced on premise and are not virtualized, or at minimum, not virtualized below high-density configurations. These service areas are also on their own tenant, not totally automated, and have significant differences across their VM installations.

To set up a visible presentation, this research provides information and information that can assist—the selection of one of the blueprints portrayed on Figures1 as the most precise expression of the connections between threats associated with conventional IT compared to cloud. Figure 1

Figure 1 Visual Comparison between Traditional IT Risks and Cloud Computing Risks



Different risks



Risks intersect

Source: Author

1.4 Research approach

The objective of this research is to obtain an in-depth knowing about the topic of Cloud Computing in requirement to make intellect of the generally threats related with cloud, and to create a structure and suggestions to reduce threats and speed up the adopting of Cloud computing. Aspect of the objectives is to postulate a design that could describe possible misalignments between real and recognized threats linked with Cloud. To accomplish these objectives, a qualitative strategy was chosen for the analysis to

analyze the "what" and "why" of cloud risks, but to assess "how" to minimize these risks.

The qualitative method depends on two standard methods: Online Questions form and interviews with subject matter experts, and the Delphi method to construct consensus. The research will analyze the trustworthiness of the information by matching the data across the facts provide by the subject matter experts.

The Online Questions form and interviews will conduct mostly in person but some interviews may will be done by phone when travel logistics could not overcome. The subject matter experts who participate in the Online Questions form and interviews it will list in end of the theses. These experts are well-known IT professionals with many years of experience and expertise with cloud computing and security.

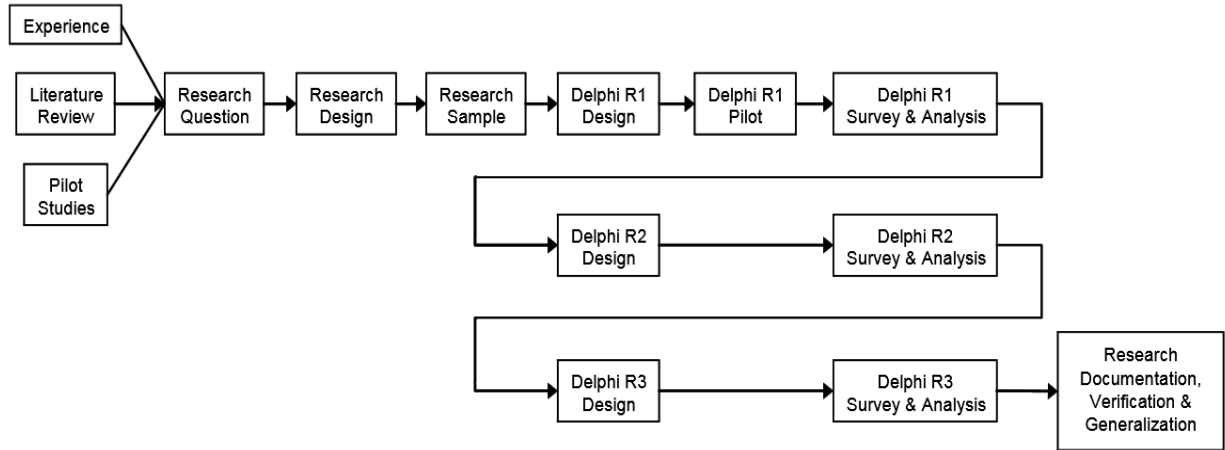
These professionals work for a variety of different industries and companies, in Czech Republic. They contribute to this research with their personal time, knowledge, and great motivation to augment the knowledge available about cloud computing. Each interview will take at least one hour long and will record using App' ITalk software. The record interviews will save and categorize on Apple iTunes under the category "expert Interviews."

The approach of using iTunes enable the cross examination of the interviews through very convenient tools like iPhone and iPad. In addition, during the interviews, many notes and diagrams will create and the information summarize immediately to obtain confirmation that the key points understand correctly.

As the interviews, progresses several patterns fast emerged and the information was feedback into the following interviews and Delphi consent structure exercises. Delphi strategy verified to be beneficial in developing bargain on solutions to issues that had no previous precedent, and in the development of new concepts like the Cloud Risk-Key-Indicators.

The Delphi process follow a structure approach on each call the experts briefer on the conclusions of the prior call and reminded of suggestions provide by other experts, thus encouraging them to revise earlier answers to gain agreement. Figure 2

Figure 2 typical delphi method



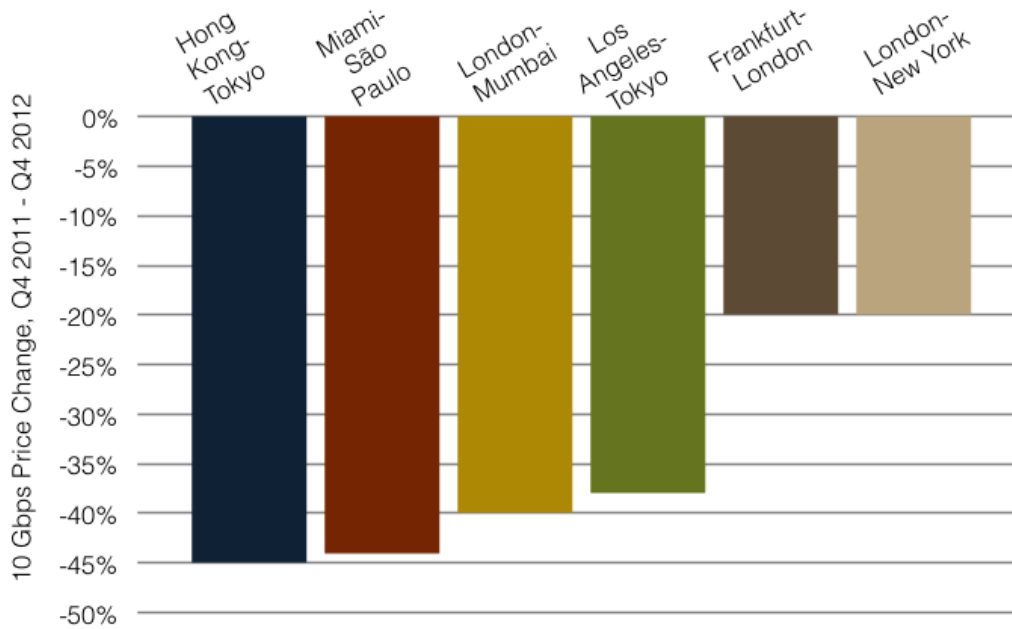
Resource: The Delphi Method for Graduate Research2007

2. Literature Review

2.1 *Cloud computing*

Cloud Computing is caused by some important market styles and commercialization of several technological innovations. One of these styles is the speeding of technological innovation adoption. The rate at which technological innovation was implemented just 100 years ago was considerably more slowly than today. As an example, the U.S. first began using radio technological innovation in 1912, and by the Twenties, the commercialization of radio began with several new shows. However, it took 40 decades for the first 60 thousand receivers sold (7). Nowadays, new technological innovation can distribute to many people to individuals in just a few short months or even several weeks. Farmville is an example of a social game that was able to distribute to 60 thousand customers in just four to a few several weeks. The speeding of technology adoption has an amazing effect on how cloud is being adopted, and how fast it is penetrating traditional IT applications. This remarkable rate of adoption of services on the cloud is driving millions of users to new mega IT centers. The method of directed computing services in extra-large IT centers creates economies of scale that further commoditize this utility computing model. However, this merging makes new weaknesses by assisting the distribution of viruses on a quicker and larger scale. An additional important pattern is the remarkable decrease in the cost of communication, which was activated by many aspects, such as better technological innovation such as optical fibers and mobile wireless, along with an oversupply of bandwidth. The cost of communication is a fraction of what it was just a few generations ago, and it continues to go even lower. For example, in most cases the median lease price of a 10 Gbps wavelength between Los Angeles and Tokyo fell 38 percent to \$25,000 per month. Prices on the more mature London-New York route fell slower, declining 20 percent to \$9,000 per month. While significant regional (8) Figure 3.

Figure 3 Wavelength Price Declines on Major Routes, Q4 2011–Q4 2012



Source: (8)

Today, the pervasiveness of cell phones provides instantaneous communication and facilitates the consumption of new cloud services or a minimal fee, or for free.

These movements have commoditized main technologies and services like hypervisors, operating systems, and computer hardware. Hypervisor technology is allows the virtualization of computer services. It has been existing on mainframes since the 1960s, but it was not until now, with the advent of open source, that Xen, KVN and VMware made this technology available on lower-cost hardware (9) (10).

The first phase in the direction of could computing, happened around 26 years ago when several computers were install together with physical wires under settings called “clusters.” These groups were firmly incorporated, purpose-built resources typically comprised of a set of web servers, changes, storage space, and system software used by only one set of users, or individual set of programs. Clusters used mainly to ensure automated of back-ups and recovery procedures, as well as for high-performance

programs that required lots of storage space or estimate power. With the coming of Personal Computer systems in the 1980's, IT options moved to a more decentralized cloud computing, and the peer-to-peer network technology created a generally combined estimate design called lines processing. These plants allow the combining of groups together, and the ability to manage these resources with scheduling and workload management software that shares these resources across multiple user groups, units, and applications. Grids enabled the creation of modularized software components that could take benefit of horizontal scaling across multiple computers, increasing the efficiency of capacities with large compute power requirements. However, grid technology was difficult to use because it required significant manual configuration and scripts.

Grid computing peer-to-peer structure trusted using nonproductive time on the participant's computer systems, and this made it quite challenging to effectively estimate the length of a particular fill demand. Lines processing was a great achievement for network sharing technology, but it failed on characteristics important to IT systems, such as automation, ease of use, and, most importantly, predictable execution time that can support SLAs. However, without the progression in technological innovation that lines processing created on peer-to-peer system emails, we would not have had the technological innovation base to advance to the next level of system automated that made cloud processing possible. The main differences between lines processing and cloud processing are defined on Table 2 (11)

Table 2 Cloud Computing Vs. Grid Computing

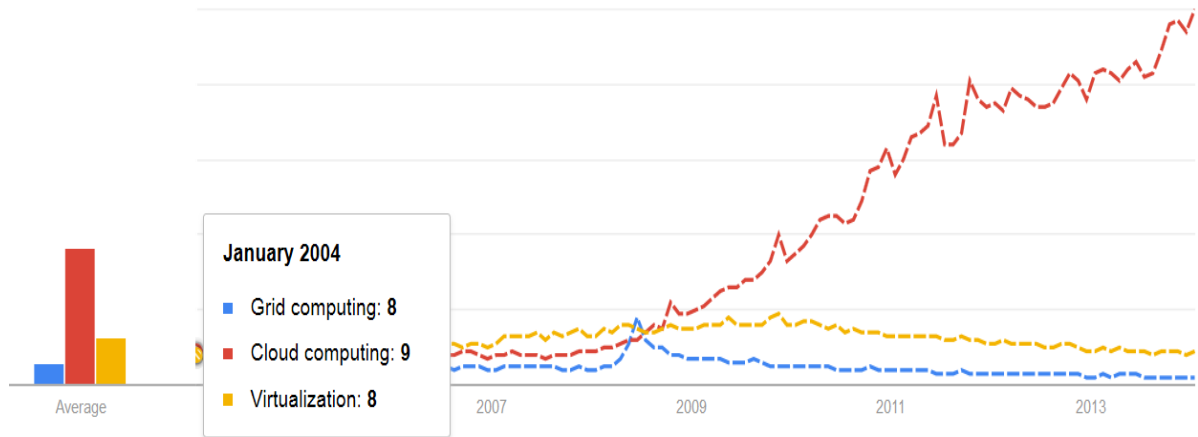
Parameter	Grid computing	Cloud computing
Goal	Collaborative sharing of resources	Use of service (eliminates the detail)
Computational focuses	Computationally intensive operations	Standard and high-level instances
Workflow management	In one physical node	In EC2 instance (Amazon EC2+S3)
Level of abstraction	Low (more details)	High (eliminate details)
Degree of scalability	Normal	High
Multitask	Yes	Yes
Transparency	Low	High
Time to run	Not real-time	Real-time services
Requests type	Few but large allocation	Lots of small allocation
Allocation unit	Job or task (small)	All shapes and sizes (wide & narrow)
Virtualization	Not a commodity	Vital
Portal accessible	Via a DNS system	Only using IP (no DNS registered)
Transmission	Suffered from internet delays	Was significantly fast
Security	Low (grid certificate service)	High (Virtualization)
Infrastructure	Low level command	High level services (SaaS)
Operating System	Any standard OS	A hypervisor (VM) on which multiple OSs run
Ownership	Multiple	Single
Interconnection network	Mostly internet with latency and low bandwidth	Dedicated, high-end with low latency and high bandwidth
Discovery	Centralized indexing and decentralized info services	Membership services

Service negotiation	SLA based	SLA based
User management	Decentralized and also Virtual Organization (VO)-based	Centralized or can be delegated to third party
Resource management	Distributed	Centralized/Distributed
Allocation/Scheduling	Decentralized	Both centralized/decentralized
Interoperability	Open grid forum standards	Web Services (SOAP and REST)
Failure management	Limited (often failed tasks/applications are restarted)	Strong (VMs can be easily migrated from one node to other)

Source: (11)

The cloud beginning was possible due to prior technologies like clusters and grid computing. Cloud computing takes grid computing to the next level by allowing end users and system administrators to schedule, organize, and manage a heterogeneous pool of compute, network, and storage resources. Additional abilities include self-service, chargeback, personalized support online catalogs, policy-based application bending and powerful provisioning across physical, exclusive, and exterior cloud resources. Compared with a group or lines, which are typically statically designed, a cloud's settings is identified dynamically depending on predetermined guidelines, and it is handled as a single entity (Table 2). In Figure 4 from google trends we can found out that how change happened through last 10 years for cloud computing.

Figure 4 change in time GC vs. CC



Source: (12)

At the central of cloud, computing is a new business model that proposals compute services on request, over a browser or remote APIs, in a very easy-to-consume format like a utility model.

The following are definitions assumed throughout this dissertation:

Virtualization - Software between the hardware and the operating system, known as the “hypervisor,” which isolates the application from the somatic box. Samples include VMWare, HyperV, HyperP, as fine as open source substitutes like XEN and KVM. Virtualization permits applications to be moveto another hardware images short of the application even “knowing.” Applications said to “virtualize” when they can be isolated to a hardware instance in this way. A current limitation of this technology is that these software solutions only work within a single hardware platform. To date there are no platform-independent hypervisors.

Grid - An application that cords together several servers with different network addresses hooked on a single logical network group. Here, the network rather than the hardware is virtualize. On a grid, servers can addressed as part of a single network, even when they are distribute around the world. The World Community Grid (12), with up to 500,000 users, is a Good an example of a grid. Community members share amount of their computer idle time for the advantage of research projects such by way of cancer, humanoid genome, HIV, and others.

Cloud Computing – An IT delivery model that serves compute, storage, and network services as a service quite than as a product, whereby virtualized shared resources, software, and information are provideas a utility over a network, typically the Internet (5). Cloud is a technology is delivery method that is meaningfully different from traditional outsourcing. Unlike the traditional outsourcing methodology, cloud computing provides standard services that can be accessed through common open protocols as web services. In traditional outsourcing prototypes, clients relinquish the day-to-day IT infrastructure conservation, but maintain control over their Requirement business processes. This is why traditional outsourcing is from time to time state to as the “Mess for Less” value proposition. To been move cloud Computing, consumers are needs to standardize to the VM conformations provided by the cloud vendor.

Unfortunately, effectiveness and price benefits obtained in the freelancing mess-for-less design are often reduce by the lack of standardization and the price of exclusive program maintenance. The IT market has become extremely aware of the improving need for speed, and the way work nimbleness is restrict by the lack of standardization. Adopting Cloud and changing Business procedures to make use of consistent Cloud services significantly decrease functional IT costs. Cloud Technology makes an elastic alternative for businesses that are Purposes to reduce cost and increase their agility. In the famed 2003 *Harvard Business Review* article “IT Doesn’t Matter,” Nicholas Carr foreseen that IT departments would finally disappear (13). We appreciate otherness with Mr. Carr and believe that IT departments will indeed survive, and will focus on core competencies that cannot be duplicate by generic cloud computing services. The

commoditization PC systems and PC solutions does not mean that the value offered by the IT division is diminished. On the opposite, IT categories will accept Cloud to decrease overall IT costs, while obtaining additional services to supplement their primary capabilities. Rather than making IT divisions. Rather than rendering IT departments obsolete, cloud will shorten and hasten the conversion of IT units. At this time, many businesses are converting their interior infrastructures to base on cloud computing technologies, but hosted privately, not multitenant, and not connected to the Internet. We will refer to this method of cloud as “private Cloud.” Many of the companies that have accepted private Cloud also usually make use of Cloud (which they refer to as public cloud) for workloads with low protection specifications. The IT divisions that accept cloud have an essentially different rental than conventional IT divisions. Instead of carefully handling a hodge-podge of programs and components, Cloud computing IT experts will focus on standard options and building alternatives based on cloud services. Imaginably most important, cloud computing helps accelerate the business transformation and keeps the business in a leadership position through IT cost reductions and limitless compute power when the business needs it.

With a knowing of the important financial benefits of Cloud, one might wonder how all this happens. What are the features of cloud, how can be fit all? How virtualization come in? Imaginably of best system to think in terms of three layers of cloud is the physical layer, the programming layer, and the services layer.

Physical layer (hardware) is heavily virtualize, allowing the cloud to maximize hardware usage by simply swap loads and moving them around as needed. That virtualization and extremely efficient load organization minimizes idle time. This layer is cover of cloud computing physical resources such as servers, storage, and network. The go to market or canal commercialization of that layer is state to as (IaaS).

Second the programming layer be made up of the APIs and programming

Is the Interfaces, which allow the writing of applications on top of the cloud, this level make available services that streamline programming for big scale IT. Some typical services include data analytics based on MapReduce or Hadoop (14), fill controlling of

VMs, and lining up services to manage large demands and still guarantee distribution. Every cloud-computing provider offers their own taste of APIs and currently there is not important interoperability across cloud suppliers due to variations on this level. This development level is from the commercial perspective generally known as System as a Service (PaaS). The layer number 3 is the (services) it is imaginably the most important level. The alternatives part encapsulates all the components, development, and system dependencies so that the customer recognizes only a simple business customer interface required to execute required everyday projects. This part is generally known as Software as a Service (SaaS) and has become popular because of the convenience it provides. Well-known SaaS illustrations are, Search engine, and popular social media.

The level of IT control changes based on the cloud part. At the IaaS the customer has complete control of the middleware and program, but associates the control of the facilities and data center to the Provider Cloud computer. At the PaaS part, the customer gives control of the middleware to the cloud company and any program designed will usually have specific rule to implement the exclusive PaaS APIs Functionality Table 3

The SaaS part relinquishes complete management to the cloud company and the customer tends to generally only management their use situations. Later we will talk about problems with the obscurity offered by the SaaS design and information problems with cross-border rules.

Table 3 cloud delivery model offers a different level of control & functionality.

Cloud Computing Delivery Model	Level of Control	Provided Functionality
SaaS	Usage control only	Access to publicly available interfaces of provided software
PaaS	Limited administrative control	Develop and deploy software and databases, with some limited control over platform's configuration
IaaS	Full administrative control	Configure and deploying virtual servers that are directly tied to virtualized infrastructure components

Source (16)

2.2 Hypervisor

The aim of cloud is an efficient virtualization development that maximizes the IT resources. But then again virtualization is nothing new. Virtual machines have been commercially existing on mainframe systems since the first 1970s, and not commercial versions VM product from IBM's have been existing since the half -1960s. The significance of this historical perspective is that virtual machine technology has existed a fundamental part of mainframe architecture for many years. The z/VM hypervisor distinguishes itself by allowing workers to host hundreds of copy of OS on an only copy of z/VM.

However, things have modified in the last 50 years, and IT has considerably progressed since the release of the IBM VM close relatives in 1972. Two aspects, however, provided to drive virtualization as a significant cloud computing allowing technology

First, massive parallel processing machines increased the difficulty of operating systems, making a variety of difficult challenges. These experiments drove innovation to simplify computer interfaces, which resulted in the creation of what we know today as virtual machines rendered by a hypervisor. There is a variety of kinds of hypervisors. Some run on top of operating system (host) and others run natively on the simple steel, but all concentrate on disassociating the components from application solutions and

developing solitude across the VMs. The kinds of hypervisors and their weaknesses are describe in part 2.2.2.

Second, the commoditization procedure of IT forced virtualization functions from high-end web servers into lower-cost computer systems. VMware is a hypervisor growth organization whose beginning rental was to make a substitute to high-end os virtualization alternatives and generate further effectiveness in after sales web servers. Other start application alternatives for virtualization are KVM and Xen, with technological innovation that can be use under the GNU certificate agreement (15) (16) (17).

The hypervisor technology and massive IT on clouds translates to the increased availability of services at significantly lower cost. The primary value of clouds— besides reduced cost is its capability to range elastically, making better accessibility and company effectiveness main to the achievements of businesses.

2.3 *Cloud elasticity*

One part that distinguishes cloud from conventional IT is its “elastic” capability. Flexibility represents the capability quickly and instantly increase the sources needed. For example, if you need more estimate power, cloud-computing can quickly spend another exclusive machine to fulfill the improved need. Huge numbers of cloud groups provide a flexibility that guarantees workloads have access to estimate, storage, and network services instantly at any time. Cloud vendors construct their cloud services slightly differently, but in general they follow a consistent cloud design that is built on large volume of high-speed, CPUs e.g. Four cores or more, 16gb of ram, and between two tb to five tb of fast ephemeral local storage. Typically 80 - 100 of servers are saved in one rack, connected with fast network fabrics i.e 10GB Ethernet or faster and from 30 - 50 of these racks are systematized and organized as one single cluster or node. In adding to the fast local storing, cluster has long-term storage in the range of one to two petabytes of storage area networks (SANs). cloud computing solutions are designed linking many of these groups across regional areas in a way that workloads and

information can be available and shifted across any place on the globe where nodes are available and offer the best system efficiency to the consumer (18) (14) (19) (20).

Group is design as an independent estimate cell appearance used as the foundation for cloud solutions. A cloud computing includes many groups, each working autonomously to maintain its solutions and to connect its position to the cloud solutions management collection, which harmonizes the overall collection of groups. This design makes great versatility for components settings to back up many different workloads in a very powerful style, offering the understanding of flexibility to the customers of the cloud. The truth is that all cloud computing have a limited potential, but the lots of potential currently available, and the allocated characteristics of the requirement for cloud sources helps provide the understanding of unlimited capacity.

2.4 Cloud reliability

In terms of 99.9999 percent to 99.99999 percent the reliability of current cloud services is measured, which funds a down time of two seconds per month or fewer. The expectation is to have access to the cloud services 24/7, but in mega IT data centers like cloud computing website hosting service facilities it is normal to regularly experience some type of problems. Cloud services are design to continue working despite these problems.

The “operations dilemma” generated by mega IT data centers that host cloud computing services was welling illustrated by Jeff Dean, Google fellow, when he said, “Even if we were to use components with mean periods. Between failures [MTBF] of 30 years and built a computing system with 10000 of those, you'd still watch one fail a day.”

When working on extensive processing solutions like cloud it is not an issue of if you will have a failure, but only when the failure will happen. A provider of cloud computing service working group is generally in a scenario where it has a 100 % possibility of a failure happening every day. However, by moving VMs around to available groups and saving information many times in different places, these everyday

problems are unseen to the customers of the cloud. Because of the flexible design of the cloud computing, clients of cloud services usually experience no actual failures of the services they use and the perceived uptime is 99.999 % or better.

Google has such an extensive search engine cloud that most users have never experienced a failure. Using Jeff Dean's data points, the Google operations team experiences failures on 2% to 4% of the servers, and on 1% to 5% of the storage media, which funds we could computing extrapolate from this and simply suppose thousands of failures each day on most clouds about the world (18). The challenge of managing large-scale cloud IT configurations is to automate and recover quickly from failure. As classic of the Google cloud Dean mentioned the following failures (18) (21)

- 0.5 overheating (power down most machines in <5 min's, ~1-2 days to recover)
- 1PDU failure (~500-1000 machines suddenly disappear, ~6 hours to come back)
- 1rack-move (plenty of warning, ~500-1000 machines powered down, ~6 hours)
- 1network rewiring (rolling ~5% of machines down over 2-day span)
- 20 rack failures (40-80 machines instantly disappear, 1-6 hours to get back)
- 5racks go wonky (40-80 machines see 50% packet loss)
- 8 network maintenances (4 might cause ~30-minute random connectivity losses)
- 12 router reloads (takes out DNS and external VIPs for a couple minutes)
- 3 router failures (have to immediately pull traffic for an hour) dozens of minor 30-second blips for dons
- 1000 individual machine failures
- thousands of hard drive failures (22)

In common, Cloud computing are long lasting solutions and offer excellent stability to their customers not because they don't have issues, but instead because they are very

excellent at determining issues and recuperating very easily from them. Cloud has comprehensive application control loads that monitor the state of the Cloud computing hardware resources as well as network traffic. The application control loads constantly do load controlling across many Cloud sets to reduce failing risks. Cloud Explicit Security Matters and Attacks

In Highest Threats to Cloud Computing, the Cloud Security Alliance said the top seven cloud risks are (23), (24)

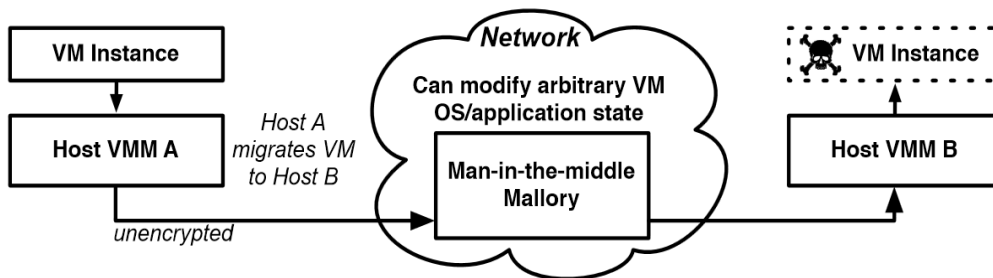
1. Abuse and nefarious use of cloud computing
2. Insecure application programming interfaces
3. Malicious insiders
4. Shared technology vulnerabilities
5. Data loss and leakage
6. Account, service and traffic hijacking
7. Unknown risk profile

In February 2013, Cloud Security Alliance has done new Cloud computing top threats According to this report the most top are: (25)

1. Data breaches
2. Data loss
3. Account hijacking
4. Insecure APIs
5. Denial of service
6. Malicious Insiders
7. Abuse of cloud services
8. Insufficient due diligence
9. Shared technology issues

Here are several strikes that are specific to cloud surroundings, such as VM browsing, following an effective hypervisor evade strike. Other exclusive cloud strikes include attacks on cloud images. Migration or movement of VMs in the cloud can be a problem if a VM is move onto a compromised network. In that situation the data in the VM can be expose to a man-in-the-middle attack. Insecure migration protocols can expose data through VMotion/XenMotion to a man-in-the-middle attack. To prevent this type of strike it is important that the management systems be individual from the cloud exclusive system to prevent possible system spying. This VM migration man-in-the-middle strike was empirically confirmed by David Oberheide at the University of Michigan (26) Figure 5

Figure 5 migration man-in-the-middle attack performed by John Oberheide



Source: (26)

2.5 Cloud APIs vulnerabilities

Cloud weaknesses another specific that has led to potential risks contains the cloud source application development connections (APIs) and interaction protocols ,An example of this weaknesses is the XML-signature-based strike that was able to control Amazon Web Services (AWS) Simple Item Accessibility Method (SOAP)messages. The vulnerability relied on the way Amazon processed the AWS SOAP message, which

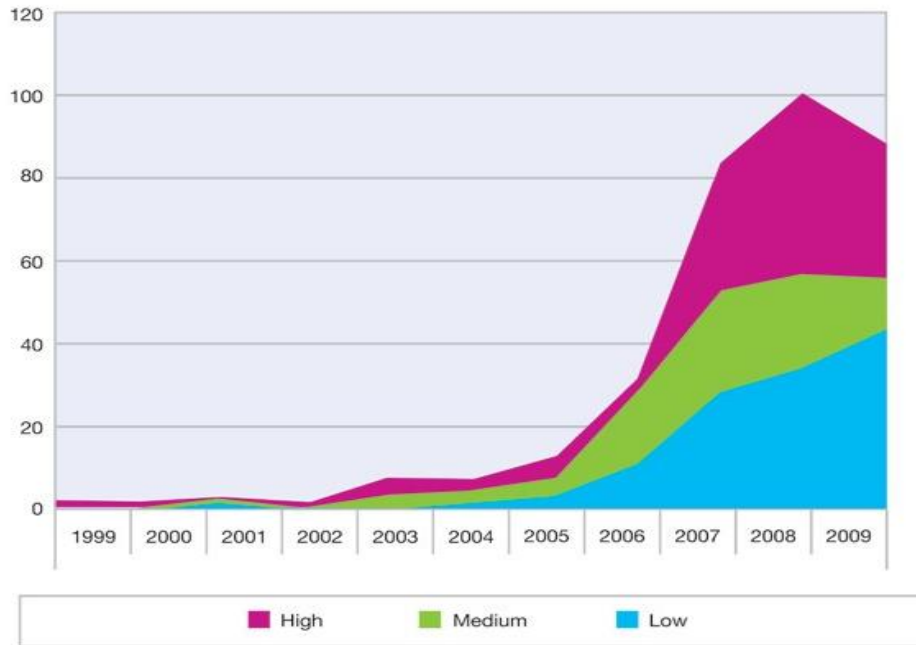
was splitting the application trademark confirmation process from the XML presentation. This separating designed the opportunity for online hackers to eliminate the finalized portion of the document and insert malicious code in its place. This vulnerability was first highlighted as a theoretical vulnerability by IBM's Paula Austel and Scott McIntosh in 2005, but was not shown practical until Oct 2011, at which time Amazon quickly set the problem (27) (28).

Eucalyptus, open source cloud remedy for personal clouds, was susceptible to the same risk but the company has stated that this issue has also been fixe

2.6 Hypervisor vulnerabilities

Unfortunately, there is many misunderstandings relevant to threats associated with hypervisor weaknesses. In this area, we will evaluation the important points around weaknesses associated with the most typical hypervisors used for well-known clouds there are many cloud components that interact with the hypervisor, so vulnerabilities are more easily understand when they are classify according to the cloud components that enable the virtualized environment. The cloud components that will be review within this section are depict in Figure (7). Note each component is characterize with a No's that we will state to during this sector. this sector the data provided about the hypervisor vulnerabilities originated from several sources together with the Intel security report from Steve Orrin (29), the Intel 2011Cloud Builders Reference Architecture (30), the *PCI DSS Virtualization Guidelines* (31), and the IBM X-Force and Sourcefire Vulnerability Research Team (VRT) 2011 security reports (32) (33) (34) (29) (31) (35). The common theme across these reports is the overwhelming evidence of serious vulnerabilities on most cloud implementations, specifically in the area of hypervisor vulnerabilities. Within the last 10 years we have accumulated a total of 373 virtualization vulnerabilities, and of those, 40 percent are of high severity, as illustrated in Figure 5 (provide by IBM X-Force) (33).

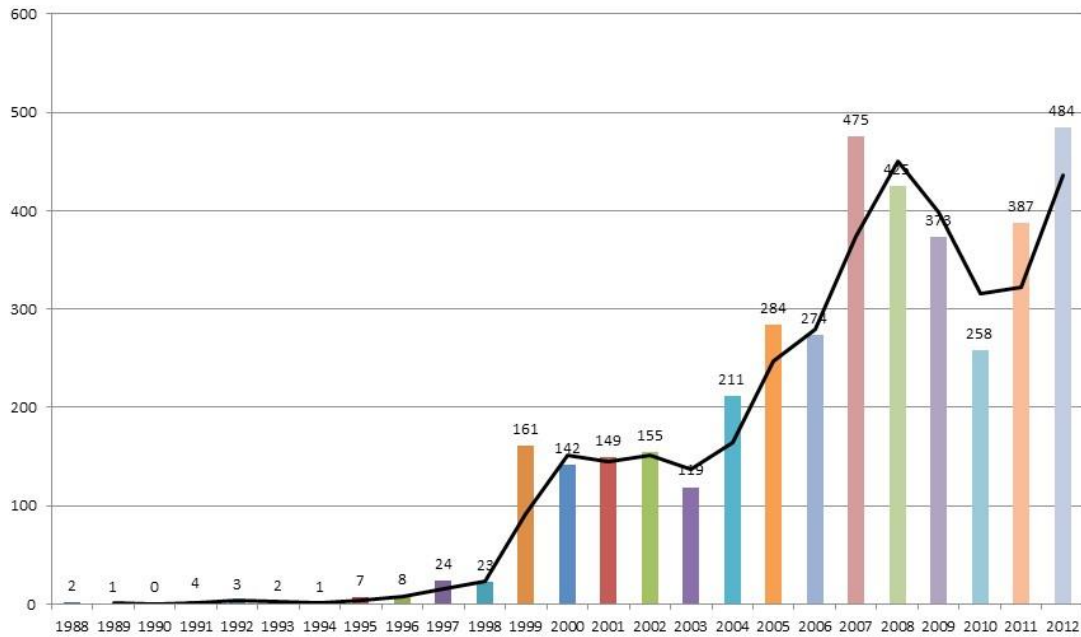
Figure 6 Virtualization vulnerability severity by year reported, 1999-2009



Source: (36)

In 2012 and according to Sourcefire Vulnerability Research Team report (VRT 2012) was for first time ever the high severity vulnerabilities only make up 33% of the vulnerabilities assigned CVEs. This a significant improvement over earlier year in the previous decade high severity vulnerabilities averaged 45% figure 6 can explain it graphically (36) and these high severity hypervisor vulnerabilities create substantial security, compliance and business risks because the VM isolation can be easily compromised, and in some instances, the attacker can gain full control of the host. Control of the host allows full access to confidential data available to other VMs within the physical server

Figure 7 Critical severity vulnerabilities by year (CVSS = 10)

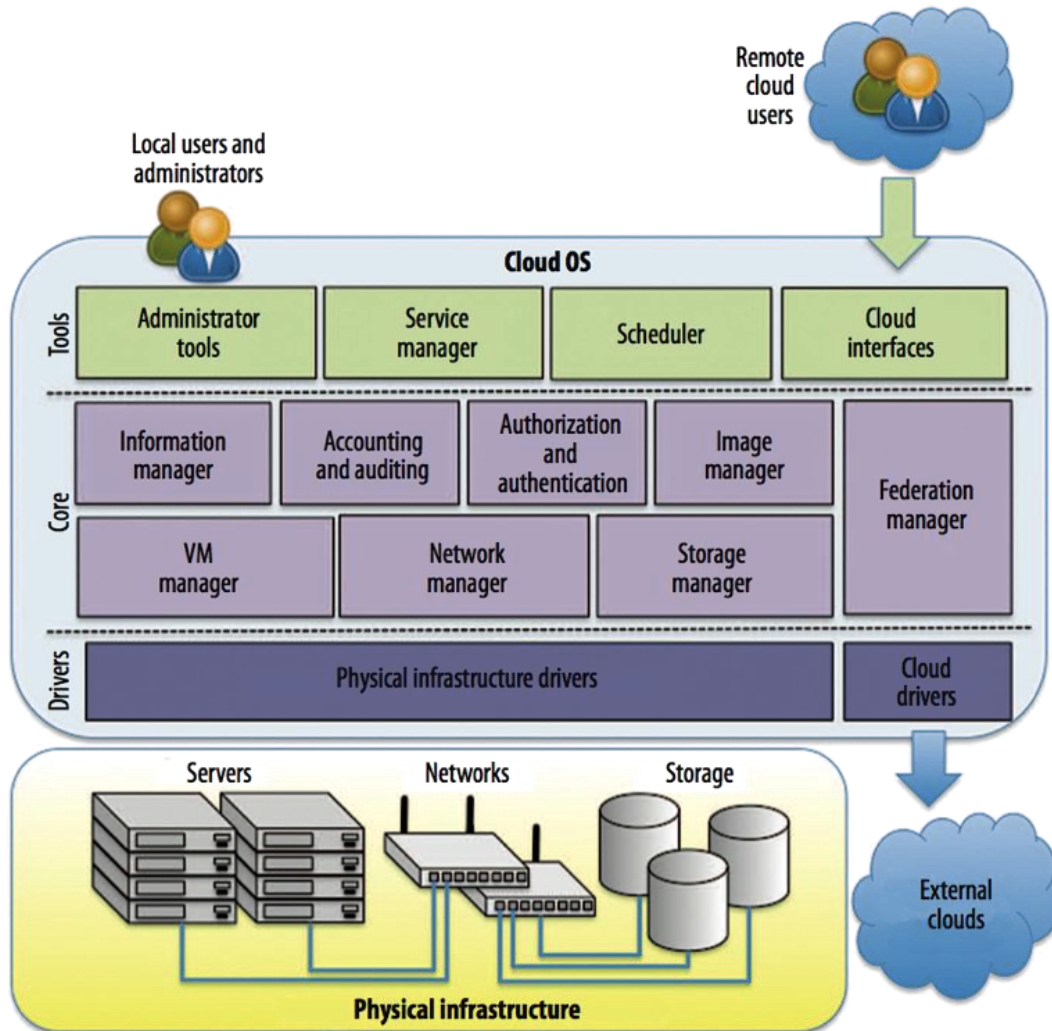


Source :Sourcefire Vulnerability Research Team 2013

Another important factor to emphasize is the place of the virtualization weaknesses. One third of the weaknesses are situated on the hypervisor application itself, but almost 50 percent of the weaknesses are linked to third-party application. This emphasizes the need to confirm and require well-defined protection analysis approval requirements before implementing application into any cloud.

In common, cloud weaknesses are due to new protection vectors, like the product hypervisors in use by many cloud suppliers. In addition, new business procedures that motivate multitenancy or multi-tenancy and unmatched range of information and estimate energy increase the threats associated with cloud.

Figure 8 Cloud virtualization components



Source: CloudCatalyst Project Officially Launched

This entry was posted in cloud, opennebula on January 9, 2013 by imllorente.

DoS attack. However, for convenience many of these consoles have been enabled for mobile access and other remote connections. The connections create security vectors common to other traditional web applications vulnerabilities such as SQL injection, remote execution of code, and blows to other control services. Since clouds negotiate

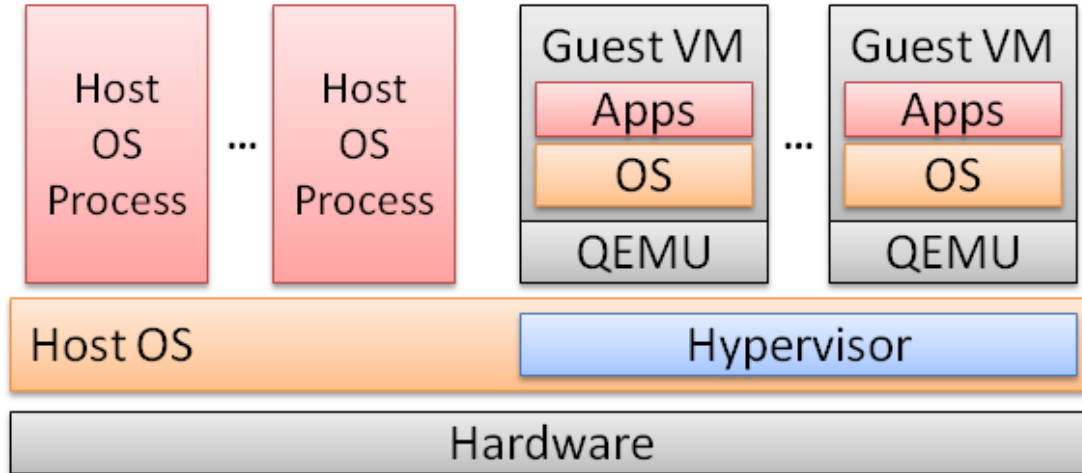
great deal of resources per control system, limiting the system can create serious issues, such as restricting the ability to perform system dash panel features and exclusive management projects that control the hypervisor settings.

The highlight of Management Server is in Figure 8 as point (2). The element that preserves the actual settings and conveys with each variety via the Administration VM to sustain the appropriate virtualization service. Vulnerabilities on the management server has known to allow the compromise the cloud configuration and the ability to run tasks at elevated privileges.

The highlight of Management Server is in Figure 8 as point 3 and is from time to time is generally known as “Dev0.” An element that controls the VMs on part of the hypervisor. This VM is also the link between the virtualized system services and the Management Server. Management VM weaknesses have involved shield flood, which allows harmful rule to run at raised benefit, accident the dom0 VM, or allow DoS on local VMs or other hosts.

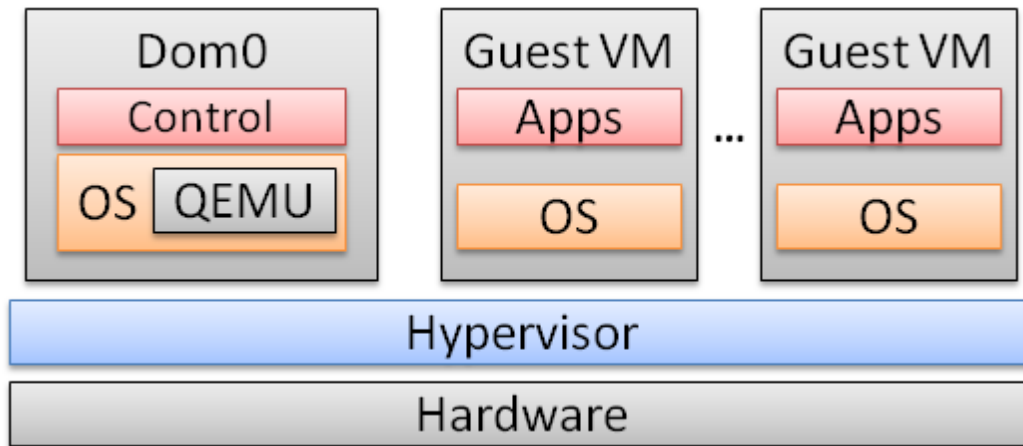
The hypervisor depicted in Figure 8 (4) is the software that virtualizes the physical host. Hypervisors are generally categorize by type. Type one hypervisors run on the bare metal and function as an operating system and virtualization manager all in one. Type Two hypervisors run on top of a wide range os and maintain a second level of indirection between wide range OS and OS & hypervisor type two hypervisors run on up of a range os and sustain a second level of roundabout between variety OS and hypervisor. Samples of type 1 hypervisors consist of zOS, Hyper-P, Hyper-V, VMWare ESXi, & Xen. Figure 10 some samples of type 2 hypervisors consist of KVM Figure 9, VMW are, and Microsoft Virtual PC Figure 9 (29) (37)

Figure 9 KVM Architecture.



Source: Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers (May 2013)

Figure 10 Xen Architecture.

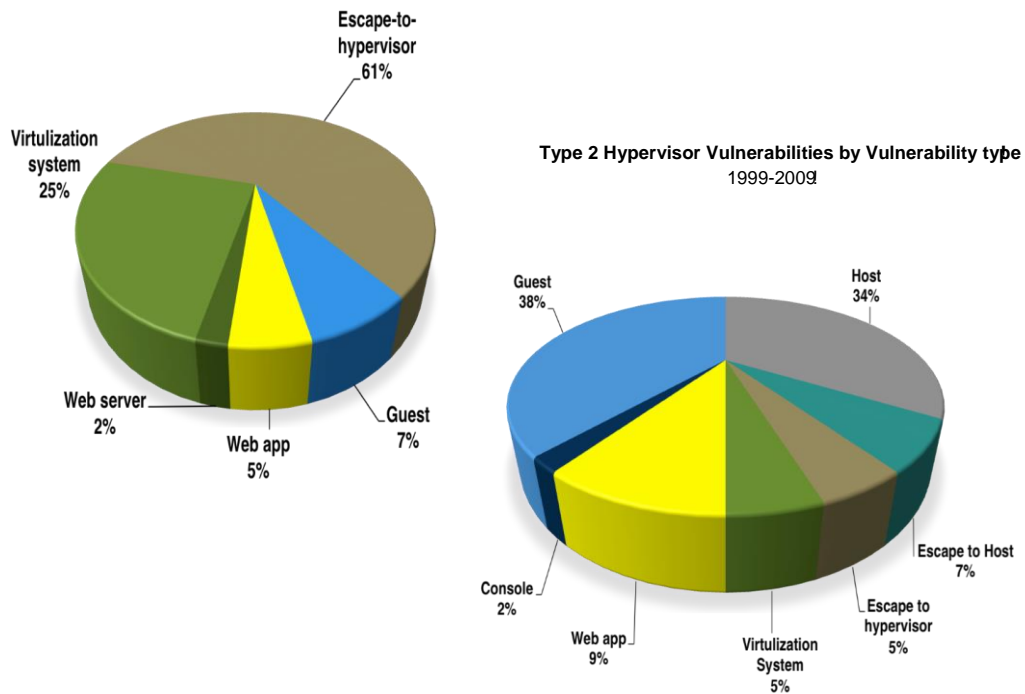


Source: Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers (May 2013)

There is many weaknesses associated with the hypervisor software part. Some of these consist of strikes that produce shield flows over to place program code that can turn off the hypervisor. Other weaknesses have been known to produce a DoS by failing the hypervisor. In addition, weaknesses consist of splitting the solitude of VMs and allowing data leak across VMs. However, the most egregious weaknesses allow quit

from the visitor VM and accessibility into the hypervisor, enabling interaction across the hypervisor to any VM organized on the actual server. The most challenging part of these weaknesses is discovering it. Because the interaction bypasses the system, there is no track produced by the strike. Vulnerabilities by hypervisor kind proven in

Figure 11 Hypervisor vulnerabilities by Hypervisor and Vulnerability types



Source: IBM(X-Force Research and Development)

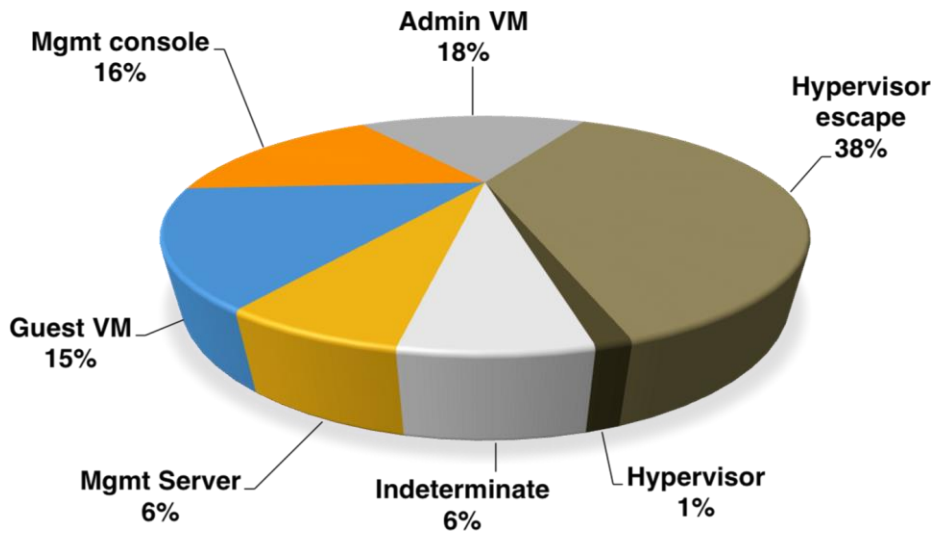
A guest VM is highlighted as (5) in Figure 7. This is a virtualized example of the actual server that runs its own OS. To the user this example acts like a regular actual server. Interaction across VMs is done through the virtual network. Weaknesses on visitor VMs include attacks where the VM can gain elevated rights, accident the VM, and generate a shield flood that allows the performance of harmful code. The Virtual Network is highlight as component (6) in Figure 7. In addition, this application makes a stage of indirection between the actual IP details and the details within the cloud. It is very important virtualize the system in the cloud to allow the activity of VMs quickly

across places, and to offer the versatility to make any taxonomy desired without limitations, depending on physical IP ranges. In accordance with the CDI 2011 mobile study (32), the most common risks associated with virtual networks are Trojan malware, malware, malware, and malware.

Moreover to the elements detailed in Figure (7), (GUI) interface user graphical portal used by cloud customers to demand new VMs, configure current VMs, manage their cloud images, and view billing statements. Sites are topic to typical web program weaknesses. Following good growth methods allows reduce needless threats to portals. GUI portals are typical across cloud suppliers. For example, the IBM Cloud provides a GUI that allows the growth a new VM with an easy three-step strategy.

According to X-Force 2010 review, guest-hopping through exploitation of a hypervisor evade is the most typical cloud virtualization weaknesses. Sixty-one % of the weaknesses of kind 1 hypervisors and thirty-eight % of the overall virtualization weaknesses were of this kind. An exciting example of hypervisor exploitation that enables a malicious hacker to escape to guest VMs is the “Blue Pill” toolkit. Designed by security researcher Joanna Rutkowska (26) four, the toolkit works as a virtual machine rootkit, to run on Windows. From Invisible Things Lab (38) we also have the “Red Pill” toolkit, which designed for AMD SVM hardware technology. Exploitation of hypervisors vulnerabilities and guest hopping has demonstrated by many researchers (39) and professionals (26) in the industry, and is one of the concerns we will investigate later under the Cloud Security Framework. The hypervisor escape is in fact the highest risk associated with the possible violation of VM isolation. The hypervisor vulnerabilities by virtual components are illustrated in Figure 9 (data provide by IBM Force) (32)

Figure 12 Vulnerabilities by Cloud Virtualization Components 1999-2009



Source:IBM X-Force Research and Development

2.7 Cross-VM Information leakage

Cross-VM attacks are a new type of vulnerability caused by the creation of a new attack surface. This attack surface was created by new hypervisors and multitenancy processes, which are used by cloud providers to create high utilization on hardware resources they rent to consumers through Internet portals. These rentals require only a simple registration process and a valid credit card number. This kind of cloud offering has an inherent vulnerability caused by multitenancy, which enables the penetration of the isolation layer without escaping the hypervisor. The technique that enables the penetration is called a cross-VM side-channel attack, and consists of the extraction of information from a neighboring VM located in the same physical host. This kind of attack extracts information from shared host assets such as memory, CPU cache, and keystroke monitoring. This attack is possible in a multitenancy environment where VMs are multiplexed on the same physical node without concern for competing companies sharing the same physical host. If a competitor decides to gain an advantage, it could possibly exploit the cross-VM side-channel vulnerability. This kind of cross-

VM side-channel attack was described and demonstrated on Amazon Elastic Cloud Computing (EC₂) by Thomas Ristenpart in 2009 (39).

The cross-VM attack consists of two steps: (1) place the malicious VM on the same host where the target VM is located; and, (2) after the malicious VM is collocated, extract the desired information from the target VM.

Dr. Ristenpart was able to obtain a 40 percent success on collocating malicious VMs with target VMs on EC₂. The vulnerability exploited for the placement of malicious VMs was the usage of sequential IP addresses on the virtual network. Using the EC₂'s DNS service it was easy to map external IP addresses to internal IP addresses on the virtualized network. However, this vulnerability on network addresses is not exclusive to EC₂. It is common across many other clouds, and the Xen hypervisor used by Amazon EC₂ is the same underlying hypervisor used by Google and RackSpace.

After the attacker knows the internal IP address of the target VM, several VMs can be created until the internal (virtual) IP address is near the target VM. To avoid a brute force approach for the creation of VMs, the attacker can first make a couple of tests to try to predict the taxonomy of a cloud. This kind of analysis can be done using WHOIS queries to figure out the IP address ranges assigned to the cloud provider. EC₂'s DNS service can be used to map public addresses to private addresses. This approach can create a very good picture of the cloud taxonomy or cartography.

After the malicious VM is created with an IP address within close proximity to the target VM, the next step is to confirm the collocation. XEN and KVM hypervisors use a management VM called "Dom0" illustrated in Figure 8, highlighted in that diagram as (3). The Dom0 management VM has an IP address assigned to it, and if the malicious VM and target VM have the same Dom0 IP address, this indicates that they are probably collocated in the same physical host. Collocation can be verified through other methods such as TCP SYN trace route. If there is only one hop from the malicious VM to the target VM's Dom0, this indicates that the two VMs are within the same physical host.

Now that we have verified that a malicious VM is collocated within the target VM, we are ready to exploit this advantageous placement.

However, there is one other consideration in this scenario. One important characteristic that differentiates cloud environments from other traditional systems that are virtualized is the “noise” associated with clouds. By noise, we mean that cloud hosts are in constant flux to optimize the hardware resources. Extracting information via cross-VM side-channels is therefore more difficult than on dedicated virtualized hardware due to three factors:

1. Unpredictable load from other VM instances collocated in the same host
2. Double indirection of memory addresses
3. Variability on CPU configurations, including some with hyper threading, making the information extraction more complex

The net result is that clouds tend to have lower extraction fidelity through cross-VM side channel attacks than traditional virtualized systems. This lack of fidelity precludes attacks that require good accuracy or large amount of bits. For example, stealing cryptographic keys through a cross-VM side-channel attack is not a viable option. Due to this limitation, clouds are restricted to coarse-grain attacks like noisy-neighbors, or stealth attacks that listen to the keystroke timings.

The noisy-neighbors attacks consist of the malicious VM scaling out rapidly and using many of the host resources to degrade the service of the target VM. This is a kind of denial of service attack but it is target at a VM. The keystroke timing attack consists of measuring the time between keystrokes made by the target VM. Using inter-keystroke times, it is possible to retrieve sensitive data like passwords.

To close these vulnerabilities, cloud providers must avoid using sequential IP addresses, and create complex algorithms to randomize the addresses in a way that is less predictable, making it more difficult to reverse engineer the taxonomy of a cloud. DNS services should be monitor for activity to avoid suspicious snooping or restrict access to only trusted parties. Cloud providers could isolate each VM with virtual LANs to close network snooping on other VMs and preclude the Dom0 from responding to TCP SYN

Treaceroute's, making the collocation test more difficult to attackers.

Eliminating or obscuring some of the tools that enable the verification of collocation could be helpful in making these attacks more difficult. In addition, some effort could be made to clear the leakage through cache wiping, and adjusting the perception of time to each VM to degrade the accuracy of inter-keystroke times.

However, while these possible enhancements require more effort and cost more money, the added security is probably worth the additional cost. However, all these efforts will only slow down the attacks rather than eliminate the vulnerability. The main issue is the simplistic approach used for registering new customers on some clouds, where just a credit card is sufficient to get a VM.

To close this cross-VM vulnerability, more thought needs to be given to where VMs are placed and whom they are collocated with. It seems that a prerequisite to safer collocation of VMs is to gain a better understanding of who owns the VMs, and implementing stricter authentication rules. This process requires a lot more overhead on the registration process, but can greatly help minimize collocation vulnerabilities. Another alternative to this cloud vulnerability is to limit your VMs to those physical hosts you paid for. This approach, however, will greatly curtail the ability to scale and take advantage of cloud elasticity, one of the great advantages of clouds.

As we have said before, security is a tradeoff between cost and risks. If you have, a highly confidential workload that cannot stand the risks associated with cross-VM side-channels attacks.

2.8 *Mobile madness*

The worldwide mobile phone market grew 1.9% year over year in the fourth quarter of 2012 (4Q12), Total shipments in 2012 were 712.6 million units up 44.1 percent from 2011 of those cell phones, and approximately 190 million will be smart cell phones by 2012, (40) with functionality that approaches PCs. The more powerful cell phones and smart tablets become, the greater the incentive for malicious attacks because of the increased amount of valuable data on mobile devices , New mobile devices mean new software, which requires time to mature. This is creating a fertile ground for malicious individuals to take advantages of vulnerabilities on mobile software. For example, the popular Skype application on the iPhone and iPod Touch makes its users vulnerable to having their address book stolen just by viewing a specially crafted message, according to AppSec consulting security consultant Phil Purviance. The vulnerability was

introduced by a new WebKit browser, which as usual was in a very early part of its maturity cycle.

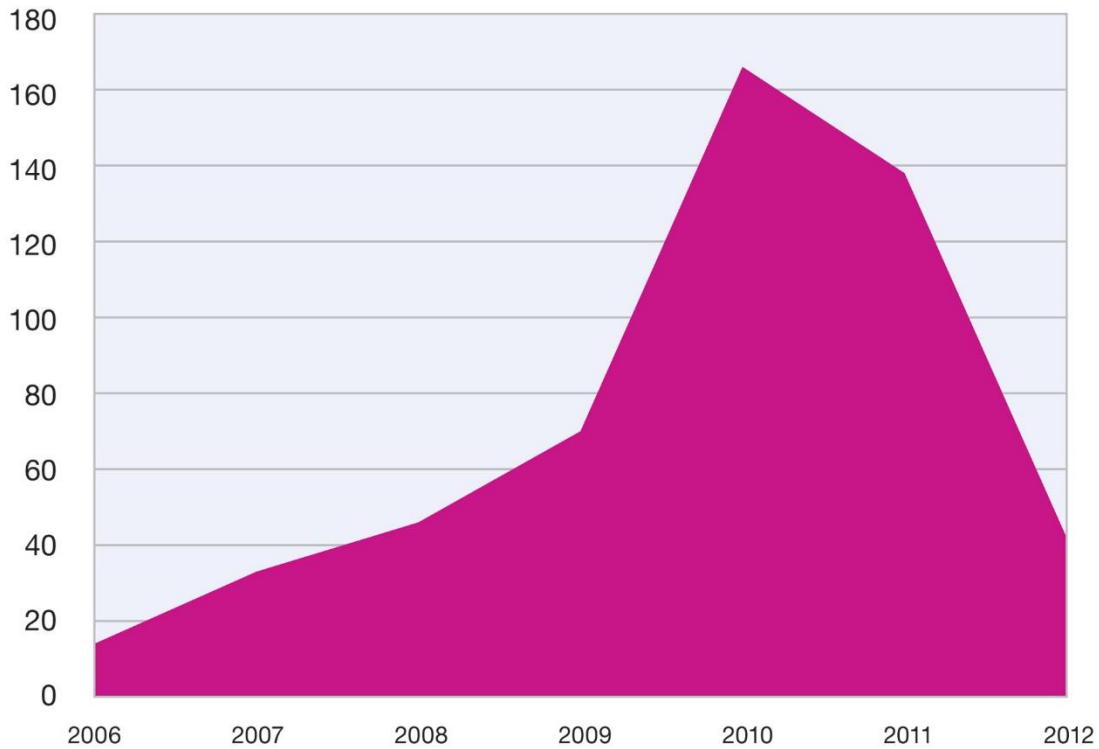
Figure 13 the worldwide mobile phone market

Worldwide mobile device shipments in 2012 and 2016 (millions of units), according to Canalys				Smart connected device market by product category (shipments in millions), according to IDC		
Type of device	2012 shipments	2016 shipments	2012-16 Growth	Type of device	2012 shipments	2012 market share
Basic phone	122.0	58.0	-17.0%	Smartphone	722.4m	60.1%
Feature phone	770.8	660.9	-3.8%	Tablet	128.3m	10.7%
Smartphone	694.8	1,342.5	17.9%	Portable PC	202m	16.8%
Tablet	114.6	383.5	35.3%	Desktop PC	148.4	12.4%
Notebook	215.7	169.1	-5.9%			
Netbook	18.3	0.3	-65.4%			
Total	1,936.2	2,614.2	7.8%	Total	1201.1m	100.0%
Source: © Canalys (Feb 2013)				Source: © IDC (Feb 2013)		
Via: © mobiThinking						

Source:<http://mobithinking.com> 2013

Smart cell phones and other smart mobile devices are experiencing security attacks similar to those experienced on PCs during the 1980s and 1990s. The majority of the attacks exploit common vulnerabilities associated with misconfigurations and poorly managed devices. However, a small percentage of the malware is “smarter” and more able to defy detection through new methods of polymorphism, stealth, and evasion. The most worrisome aspect is that 94 percent of the 8,562 vulnerabilities detected in 2010 were remotely exploitable, making the endpoint devices a potential outlet to malicious or abusive behavior. Of these 8,562 vulnerabilities, 166 were mobile phone operating system specific Figure 14, and those have many well-known exploits documented publically

Figure 14 Total Mobile Operating System Vulnerabilities



Source: IBM X- Force research and development 2013

The two main drivers affecting the increased vulnerability of mobile phones are the addition of new mobile operating systems and the increase of smart phone applications. As more applications become cross platform, they bring with them their vulnerabilities, and facilitate the propagation of malware to the clouds that support these devices. It is important to keep in mind that to decrease cloud risks we need a well-managed endpoint process to reduce mobile vulnerabilities.

Basic endpoint management recommendations:

1. Install security technology like anti-virus on all endpoints, including smart phones.
2. Use an asset manager that can enforce software policies on endpoints and track configuration as well as data on all devices regardless of their location.
3. In case advice is stolen or lost, ensure there is an ability to reset or wipe sensitive and confidential data.
4. Patch endpoints early and often.
5. Monitor behavior, network traffic, and other software patterns to identify outliers that could indicate system compromises.
6. Educate employees on endpoint policies and empower them with tools to easily update their devices.

2.9 *Human Factors - the security weakest link*

Cloud computing has accomplished many technological advances, especially around automation. However, even today the weakest link in security and compliance risks is the human factor (41), either intentionally caused by, for example, a disgruntled employees, or accidentally by a simple human error. According to the 2012-2013 Kroll Annual Global Fraud Report- a survey of 800 senior executives Around the world — 67 percent of fraud activity was committed by insiders, up from 60 percent in last year and 55 percent in 2010 (42)

Unfortunately, cloud technology does not help with security breaches and compliance failures related to weak password protection such as writing the password on a piece of paper somewhere on the computer. However, are there any other scenarios where cloud computing could have an impact? More specifically, how is cloud computing affecting the human link?

Are clouds creating more unintentional human errors?

It is difficult to quantify the actual effect of human error on clouds since coordinating a control experiment of the same users and IT administrators before and after using cloud technology is difficult, if not impossible, to conduct. However, a thought experiment can help analyze the risks and explore the potential consequences of cloud technology on the human link.

Cloud computing are highly automated and complex systems with large amount of compute, storage, and network bandwidth. Automation technology perhaps has reduced the amount of work for IT administrator and as such, has reduced the surface for error. However, we need to make sure we are comparing apples to apples. For example, what is the difference in IT capacity between traditional IT administration and cloud? Looking at IBM and Amazon as examples, we could safely say that cloud brings two orders of magnitude between traditional IT and cloud. Automation enables IT administrators to control and manage a larger number of servers, and as a result, there are fewer administrators per hosts in mega data center than in a traditional IT environment. Given the high density and large amount of compute power the cloud administrator handles, we cannot give much credit to automation in mitigating human error.

Can accidental human error still happen in highly automated environments like the cloud? Unfortunately, the answer to this question is a resounding yes. In fact, this research will try finding, through a qualitative interview, process how experts strongly agree with when the things go wrong in the cloud the massive capacity of the cloud tends to magnify most problems. In addition, automation sometimes works against the IT administrator by propagating problems faster. A very good illustration of this problem is the 2011 Amazon re-mirroring storm.

On April 21, 2011, Amazon was doing a routine upgrade of one of their routers connected to one of the Elastic Block Storage (EBS) systems, Amazon's EC2 block storage service. During the upgrade process, unfortunately, an unintentional human error was made on a router configuration. The Amazon engineer accidentally routed high capacity networks to secondary backup network services. This created a situation

where many hosts were stuck in loops trying to replicate their data to the new secondary backup network, in what is called today the re-mirroring storm scenario. (43)

This re-mirroring storm affected numerous companies that lost data and went down for 18 hours, and in some cases for more than a day.

It is important to point out that this mirroring storm is an isolated case and not an inherent problem with the Amazon cloud architecture or technology. However, it serves to illustrate that like any other software; cloud automation has bugs and weaknesses and is not bulletproof. Looking at the record of accomplishment of cloud automation event failures due to human intervention, we have to conclude that these events occur very infrequently, but when they happen, the results can be dramatic in magnitude and consequences. From the automation, perspective we would have to conclude that cloud computing has increased the risks associated with the magnitude of accidental human error.

However, what about intentional or malicious attacks by insiders? Security breaches usually happen because a person with critical access has been paid a bribe to get sensitive data. But, what impact does cloud have on this behavior? We could argue that attacks are usually motivated by financial rewards. The more pervasive clouds become the more financial rewards they could potentially generate. Seventy-five percent of the experts interviewed by this research agreed that cloud mega data centers create value concentrations that can generate higher risk than in traditional IT. In addition, as companies migrate to cloud services, the risk of intentional attacks by insiders will migrate from traditional IT to the cloud.

The consensus from the experts was that clouds pose some additional risks due to the density associated with thousands of hosts and businesses running within the same cloud hardware that is managed by only a handful of people. In the cloud environment, the compromise of a single IT administrator can be far more damaging than in a traditional IT environment, where businesses run on independent and dedicated hosts with low Utilization and density.

Fortunately, due to the standardization in clouds and the concentration of hosts controlled by the management console (explained in section 2.2.2), it is significantly easier to monitor the behavior of cloud system administrators. There are many monitoring software packages that can track the behavior and activities performed by the system administrator to assist in the identification of suspicious patterns and outlier actions. The results of this active monitoring are alerts that can warn superiors of possible risks. Monitoring software for cloud management consoles tracks not only the activities but also associates the transactions with the administrator's ID for easy determination of problems and accountability about who did what on the cloud, and when they did it. This kind of monitoring software is available for a relatively low cost, and provides a viable alternative to reduce part of the cloud have increased risk due to value concentration. Monitoring software tends to be somewhat effective because criminals are sometimes frightened, by the possibility of being identified for their illicit acts. Taken together, based on the factors considered for this evaluation, unintentional human error seems to be higher for cloud computing than for traditional IT. This is not a surprising conclusion since most new technologies confront substantial human errors until maturity brings better designs that minimize or reduce the most common problems that tend to cause human error.

2.10 *Compliance and regulations*

Many of the new regulatory compliance mandates, like the Sarbanes-Oxley Act (SOX), bring greater transparency and value to the free markets, but at the same time have created many changes to the internal corporate governance and financial practices, which have resulted in higher complexity of IT solutions and operations. For example, the periodic statutory financial reports required by SOX include many new checkpoint reviews and certifications. Given the dynamic business environment most of us live in, the current complexity of international/cross-border business transactions, and the numerous intertwined business relationships across corporations, it is sometimes is

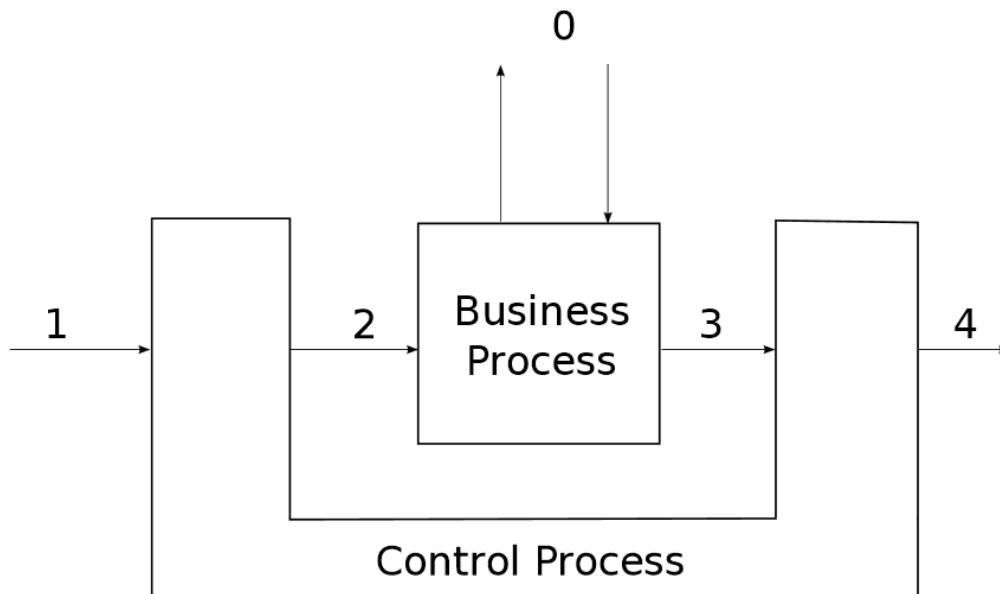
difficult to keep up with the regulatory compliance and adhere to the many new security requirements that are part of SOX.

To encourage a spirit of increasing corporate transparency, new regulations have imposed rules that require businesses to report any transaction that could affect financial statements such as off-balance-sheet liabilities and obligations. In addition, corporations must publish the internal business procedures they are using to ensure compliance and accurate reporting of financial data. Any noncompliance must be fixed within 90 days to avoid penalties or fines and/or up to 20 years imprisonment for inappropriate financial reporting and handling of documents. In addition, these new compliance regulations have increased the amount of digital data that corporations need to retain, secure, and make available for audit, in case a court subpoena requests the information. Data expected to be provided by businesses during a court order or compliance audit includes usage history of IP addresses, transactions logs, email, phone calls, data required to replicate the IT environment, and text messages sent or received by employees. Unfortunately, complying with regulatory mandates creates significantly more work for IT departments that are required to maintain the access controls and retention of all this sensitive data. Hefty penalties for noncompliance have encouraged businesses to get serious about adhering to compliance requirements.

Some businesses are more affected than others are by an increase in regulations. Financial companies, for example, specifically banks, need to comply with Basel II (2004), which imposes greater regulatory compliance on financial risks. This regulation requires tight monitoring of financial risks on lending and investment practices to offset those risks with sufficient capital reserves. What this means is that the greater the risk to which a financial institution is exposed, the greater the amount of capital it will need to hold to maintain its solvency and overall economic stability. The Basel II and III (2010-2011) mandates require substantial IT enhancements to achieve a dynamic investment monitoring and forecast mechanism to maintain financial risks within regulatory mandates.

To adhere to these new governmental regulations some of the methods recommended by experts on compliance include following three steps (44), 15, (45) (46)

Figure 15 Channels between control and business processes



Source: GoCoMM: A Governance and Compliance Maturity Model 2012

- **Step 1:** Perform preliminary and informal reviews of internal business processes and corporate data security controls. For example, check for the existence and completeness of key documentation such as the organization's information security and risk policy. Ensure IT leaders and required personnel are familiar with the audit process and regulatory compliance procedures.
- **Step 2:** Establish regular detailed and formal compliance audits, independently testing against the requirements specified by key regulations. Regularly audit IT procedures and IT personnel responsible for securing and maintaining financial data. Document security procedures and tools to maintain appropriate

access to confidential/sensitive data, provide accurate financial records, and maintain safe IT operating procedures. Documentation of standard security procedures is the best way to demonstrate commitment to quality of information, minimize audit hiccups, and accelerate achieving compliance.

- **Step 3:** Compliance requires constant monitoring, and without automation, this can become expensive and unsustainable in the long run (44). After documenting the business procedures and understanding the most important risk scenarios, it is of great value to automate the business processes, leveraging IT tools and corporate data, to help correlate possible new risks and highlight irregularities.

Step 3 is where new technologies as if cloud standardization and cloud automation scripts could help achieve compliance with less human intervention and at lower cost than traditional IT. In other Chapter for Cloud Compliance Risk Framework, we will discuss the findings of this research, illustrated by experts' comments and opinions about cloud compliance risks, and the possibility of leveraging cloud automation scripts to reduce the compliance risks associated with cloud environments.

2.11 Other efforts engaged in cyber security

On the positive side there is an enormous amount of effort that ethical hackers are doing to identify malicious software and create tools that can provide early detection before contamination spreads on highly populated IT environments like cloud computing. For example, ethical hackers around the world are working on competitions like Cyberlympics (14) to spread the knowledge and awareness of security risks and fight against organized attacks.

Governments around the world are recognizing the threat of cyber-attacks and the implications of having cloud services and mega IT data centers resident in their countries. For example, Singapore is strategically located in Asia with great network access, plenty of highly skilled IT resources, and a well-established, business-friendly government friendly. These conditions appear to have created a big influx of mega IT data centers in Singapore. Companies like IBM, EMC, HP, and KDDI have created

mega IT data centers in Singapore to host their clouds services for the Asia markets. In support of these new IT investments and threats to large cloud hosting centers, the Singapore government in 2011 began setting up a National Cyber Security Center to help counter cyber-security threats and to make the overall government more effective at reacting to cyber-attacks on local cloud hosting services.

Now that we have a good understanding of cloud computing and current vulnerabilities, we can take some time to explain the methodology followed by this research, before moving to the findings. The next chapter will review the research methodology systematically, and will compare the classical Delphi process with the modified Delphi method used by this research to provide a more agile consensus process.

3. Research materials and methods

3.1 Qualitative method

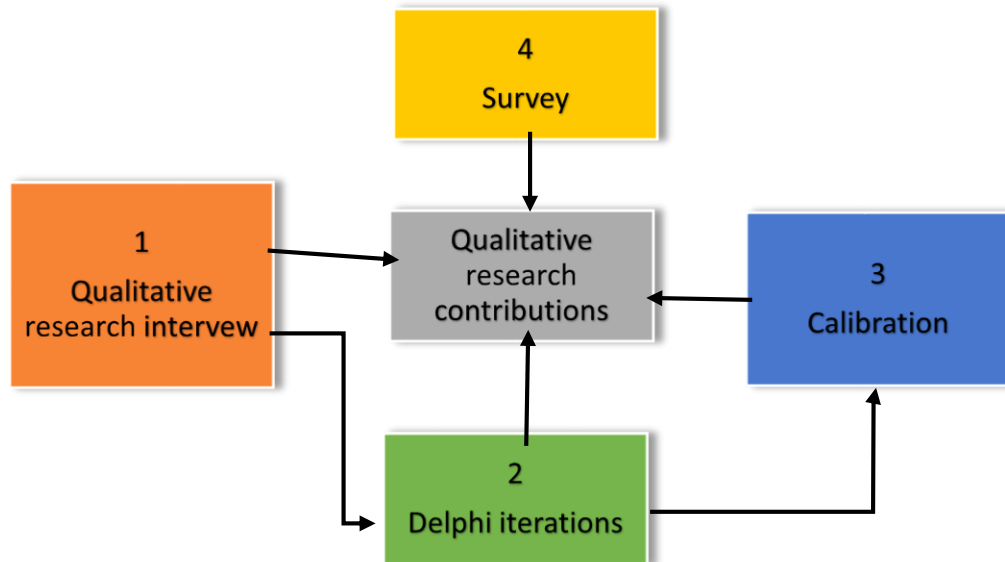
This research analyzes many cloud-computing issues related to security, business, and compliance in an attempt to make sense out of the risks associated with these complex systems. With this qualitative research, we attempt to answer the “what” and “why” of the most important cloud risks. It has left for further research to determine the “how” to best fix cloud problems identified by this research. This research is achieve a simple and coherent way for IT manager to understand and rationalize cloud-computing risks and help them gain some insight on reducing strategies for current cloud risks.

This research used several instruments to research and evaluate risk vectors associated with current cloud computing offerings, and then compared those risks to traditional IT. In the context of this research, as we discussed in Chapter 2, Traditional IT refers to an IT environment that not virtualized, not multitenant, hosted on premise, and with minimum automation. Traditional IT is a well-understood model and that is why is select as the frame of reference to compare with new emerging cloud services risks.

The method employed by this investigation used multiple techniques to collect data, test with a control group, and refine questions as more knowledge gained on the subject.

This research using a modified Delphi process that consisted of Online Questions form and interviews, Delphi iterations to build consensus, and a quantitative analysis that was built using a calibration spreadsheet. These three steps depicted as boxes 1, 2, and 3 in Figure 14. In addition, this research conducted a survey with IT professionals to gain additional support regarding cloud risks perceptions. This research step illustrated in Figure 16 as box number 4. The final research deliverables listed in the last box in Figure 16

Figure 16 Steps followed by qualitative research



Source: Author

Four main steps were follow by this research:

- 1) Online Questions form and interviews with cloud and security experts across different businesses. This group will be referred to as the “experts” in Appendix B the online form it will be create with Google form including the 6 questions the length of the interviews ranged from one to two hours. The interview process spread out over three months because scheduling logistics were often difficult given the very busy schedules of these experts. The interviews will record by using ITalk, stored in iPhone, and play via the iCloud on several devices that included iPhone and one iPad. The replay of the audio interviews made

very convenient by the iPhone, which facilitated the frequent review of the interview material at home.

- 2) The modified Delphi process gained consensus through five consecutive iterations of consensus-building exercises, which will conduct in phone meetings when not possible to have face to face interview with some of the experts. The Delphi iterations will conduct with 4 experts. The meetings will conduct as short consecutive conversations about specific topics to drive agreement on cloud risk vectors, the evaluation of cloud risk compare to traditional IT risks, framework taxonomies, best workload for clouds, and reducing strategies. A total of experts participated in the Delphi iteration exercises. This collective will be refer to as the “control” group for the purpose of other tests. The Delphi process will consume between (2-3) months to obtain consensus about the cloud risk vectors and framework taxonomies.
- 3) As part of the Delphi method, we quantified the cloud risk vectors using a process we designated as the “calibration” cycle. This process took place over a six-week period, during which the results from the Delphi efforts and insight from the one-on interviews were put together to obtain agreement among of the experts. This process used a spreadsheet instrument to collect the opinions and perceptions of experts regarding the risk vectors that composed the Cloud Security Risks Framework, Cloud Business Risks Framework, and the Cloud Compliance Risks Framework. Also, in this validation process the experts will ask to provide their feedback and opinions on workload affinity with cloud environments, diagrams with multiple risk taxonomies, and, using a pyramid paradigm, to rank the top eight cloud risks compared to traditional IT.

- 4) After the modified Delphi process will complete, a survey will conduct to test and compare the risk perceptions and opinions of the experts with a larger population of IT professionals. The target audience for the survey was IT professionals with several years of experience, but not necessarily experts on cloud security. The survey content and process described in section 3.2. The four steps used by this qualitative research are depicted in Figure 14 with arrows showing how the input of each process was used in subsequent investigations and evaluation

Qualitative investigations tend to collect significant amount of data, and this research will collecting over audio, video, presentations, reports, diagrams, papers, database, email communications, and statistical data on cloud security. Leveraging the power of cloud, this research stored all the data on Sky Drive and Google Drive a storage cloud service that after answers cloud and security experts and collecting a significant amount of data from many sources, the analysis of the online form and interviews was challenging. Significant effort was required to condense the key risks and reducing recommendations from each expert. Due to the broad range of experiences and different risks share by the experts, it was necessary to gather consensus to simplify the information, make sense of its significance, and construct a way to normalize the risk vectors that appear consistently during the interview process. A modified Delphi method was implement to help streamline the process of consensus building. The details of the modified Delphi research process used by this research and its comparison to the traditional Delphi process is discuss in the next section.

3.2 *Delphi research process*

Delphi method Is a technology continues Organization, it was originally developed as a method of prediction methodology and interactive rely on a panel of experts. Where the experts answer questionnaires required, envisioned the subject in two rounds or more, after each round, the broker sends an anonymous summary, contains a summary of the expectations of experts, from the previous round and the reasons that were built based on their judgments. Thus, experts are encouraged to review their answers in the light of the previous responses from other members of the Committee of Experts. The name "Delphi" derived, from the Oracle of Delphi, a figure from Greek heritage. Delphi method, developed at the beginning of the "Cold War", to predict the impact of technology on the war (47). In 1944, General Henry H. command. Arnold generates a report for the US Air Force, for the technological capabilities in the future that might be used, by the military. The Delphi method is a popular research methodology for doctoral dissertations (48). The methodology is suitable for research, efforts that are trying to increase the understanding, of a problem and to gain insight from the experiences of early adopters. Of new technologies, like social networks, and wireless phones (48). This research selected a Delphi methodology because we were interested in finding qualitative measures and understanding around cloud computing risks by leveraging the knowledge of cloud experts and other cloud early adopters. The Delphi method has been successful with research problems where there is incomplete and scarce information available (49). In addition, this research methodology has shown to be effective where precise analytics is not applicable, and the analysis of the subjective judgment of individuals as a group or collection of experts is the best available source of information (49) one of the advantages of the Delphi method is that opinions tend to converge on successive rounds of feedback. (50)

The Delphi methodology provided an effective approach to create agreement among cloud experts. Through five rounds of guided questions and feedback, we were able to gain consensus about the cloud risk vectors when comparing them to the risks associated to traditional IT. In addition, the consensus process gained agreement on the taxonomy to use to represent the cloud risk vectors. Using a pyramid paradigm, the consensus process also led to agreement about the ranking of the top cloud risks to express the relative risks compared to Traditional IT. To fit the needs of this research the classical Delphi methodology updated to create a modified Delphi method that helped streamline the consensus process. We will highlight the differences between the classical and the modified Delphi methodologies, but first let us review what we mean by classical Delphi methodology. The classical Delphi process defined by Norman Dalkey in the 1950s and later revised by Rowe and Wright in 1999. It is characterized by the following four aspects (51), (52).

1. Anonymity of Participants – This enables participants to feel free to express themselves, experience no inhibitions, and avoid external pressures. Ideas is evaluate based on their merits instead of who provided the idea.
2. Iterations – Multiple rounds of consensus building exercises provide many opportunities for participants to refine their ideas. Classical Delphi usually uses three iterations.
3. Controlled Feedback – Information and opinions of other participants are provide as controlled feedback to participants to drive consensus.
4. Statistical Aggregation of Group Responses – This enables the statistical evaluation and interpretation of data.

We did not follow a classical Delphi process; however, the four characteristics were satisfied using an innovative approach that made some slight updates to the methodology. The two main differences between the classical Delphi process and the modified Delphi process followed by this research are (1) the grouping of participants and, (2) the way statistical measurement was achieved. The first step of the modified Delphi method was the creation of the research questions used during the Online Questions form and interview process. The research questions were discussed in Chapter 1 and listed in Table 1. The second step in the modified Delphi method was the selection of cloud security experts with significant experience with an understanding of the possible cloud risk vectors. The selection of the experts was a relatively short task because we had access to many cloud experts within IBM and other cloud companies. This research used a substantial size of experts, who will be subjected to thorough interviews in which they will ask the standard research questions, along with other questions based on their expertise. The third phase of the modified Delphi method will conduct the Online Questions form and interviews and Over a person

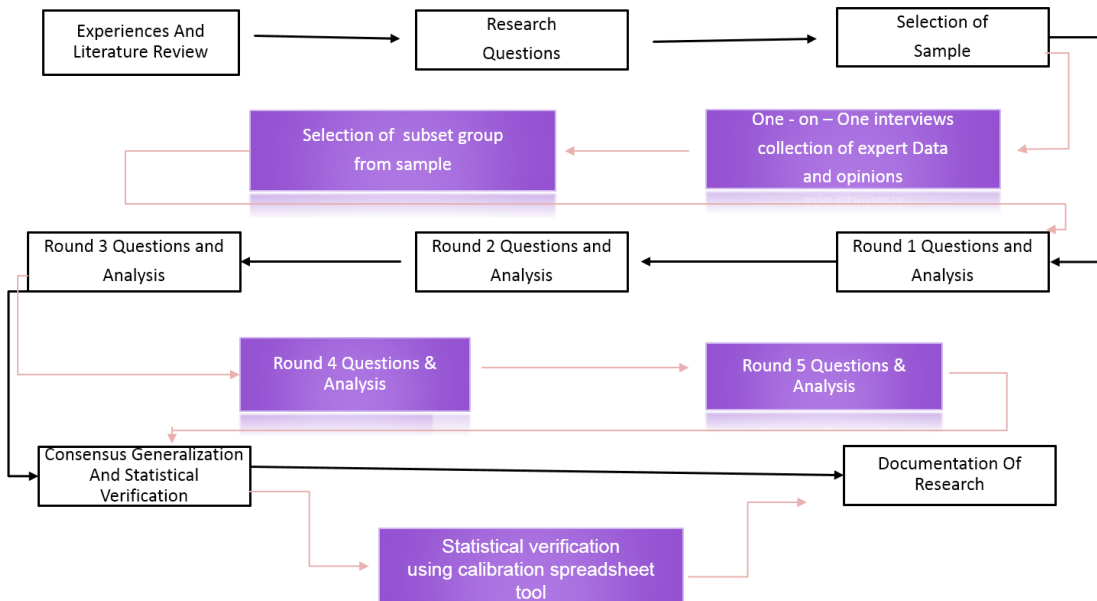
Substantial information was collected that required categorization, analysis, and substantial rationalization. The output of the interviews consist of a collection of cloud risks, suggestions of reducing strategies, and personal experiences with cloud technologies. The Online Questions form and interviews generated many cloud risks and revealed that the experts had different ways to refer to the same risk. Very quickly, the need for a taxonomy to normalize the cloud risks became apparent.

The outcome of the Online Questions form and interviews required vetting and refinement but the logistics associated with conducting iterative reviews with experts was too complex. Instead, only four of the experts were selected for this process. The fourth step of the modified Delphi method was the iterative consensus-building process. For these exercises, we used a subset of the experts. The use of only a subset of the interviewed population to gain

consensus is one of the main differences between the classical and modified Delphi methodology, the modified Delphi Figure 17. iteration process provided two advantages. (1) it collected more expert information since the target sample of experts interviewed for this research is relatively large compared to other classical Delphi methods (48), and (2) it simplified the logistics of scheduling many rounds of calls and meetings since the sample size for the consensus exercises was relative small compared to the sample interviewed. Trying to schedule iterative rounds of discussions with very busy experts was almost an impossible task and that is why a subset of the experts was select to distill the information and gain consensus.

After gaining consensus, the last step on a Delphi method is to provide some level of statistical verification. This is where another difference exists between the classical and the modified Delphi methodology. We conducted the statistical verification with the total population interviewed during the Online Questions form and interviews instead of only with the small population that participated in the consensus building. Traditional Delphi method collects statistics through subsequent questions sent to and discussed with the participants.

Figure 17 the modified Delphi



We followed a different approach because the massive amount of data received through the Online Questions form and interview process required a more flexible way to drive consensus. Reducing the number of experts in the consensus exercises provided a significant improvement in the manageability of the consensus task. However, we still wanted to verify the consensus obtained with the subset of experts with the larger sample of experts. To do this we added the calibration process, which uses a calibration spreadsheet tool to collect input from the experts and enable the statistical aggregation of the responses. This statistical aggregation use to verify the cloud risk vectors' relative threat when compared to traditional IT. The calibration tool explain in the next section.

3.3 Calibration process

The purpose of the calibration process was to gain understanding about the level of agreement that the experts would have on the frameworks constructed through consensus driven exercises with the control team. The calibration process dived into four Steps:

1. Creation of a calibration instrument using an Excel spreadsheet.
2. Test instrument with subset of five experts to ensure clear understanding of the risk vectors on each of the frameworks.
3. Collection of votes and additional observations from the number of experts through the calibration instrument and email exchanges about the risks vectors, three framework taxonomies, and a diagram depicting the cloud pyramid of risks to facilitate the prioritization of the top cloud risks compared to traditional IT.
4. Consolidation of the votes from the 4 experts who provided feedback in a single spreadsheet to tabulate votes and analyze results.
5. Construction of a diagram showing percentage tally of votes for easy evaluation and correction of any disagreement between experts and control group.

The calibration instrument built using an Excel spreadsheet following the same taxonomy used for CSRF, CBRF, and CCRF, which be described in later. Each of the risk vectors that influenced the components of the frameworks were listed with four radio buttons labeled, “Increases Risk,” “No Change in Risk,” “Decreases Risk,” and,

“Don’t know.” Each of the comparisons refers to the effect that the vector has on increasing or decreasing risk in cloud computing compared to traditional IT. The final answers on the radio buttons, recorded with values ranging from one to four, were record in the Response column (or G column of the spreadsheet) for easy extraction and collection of votes on a single spreadsheet, to facilitate counting the votes and performing the analysis step.

3.4 Survey

In survey part, we will describe the survey questions and the process that used by this research to gain insight about cloud risk perceptions. online form and interview process with experts are will try to find out if there is any contrast between cloud computing experts and the majority of other IT professionals regarding their cloud risks concerns. This section describes the questions that will use to conduct the survey, explains the underlying hypotheses, and the relationship between the questions. There are two hypotheses for which we are trying to find supporting evidence using this survey:

3.4.1 Research hypotheses

Hypotheses 1- There are differences in risk perceptions between cloud security experts and other IT professionals who are not subject matter experts.

Hypotheses 2- Deep knowledge of cloud security can have a conservative effect on the adoption of cloud services.

Also, this survey will construct to provide further evidence about data already observe during the qualitative online form and interview process regarding the best workloads for clouds, and evaluation of the cloud readiness for mission-critical workloads.

This survey was inspired by the work of Dr. L. J. Camp, and it follows a similar survey approach established by Dr. Li-Chiou Chen and Dr. Daniel Farkas in their paper, “An Investigation of Decision-Making and the Tradeoffs Involving Computer Security Risk” (53) (54). In that, paper a scenario depicts an ecommerce transaction reward, such as a discount on a purchase of a camera, if an unknown script is download to the customer’s computer. In this survey, we follow a similar approach by asking two

questions that measure the level of cloud adoption based on scenarios that test the participant's information about protection and conformity threats. The following are the two concerns developed to evaluate the cloud adopting tradeoffs with protection and conformity risks:

1. Assume you are an IT manager responsible for deploying a new Customer Relationship Management (CRM) solution. Which option would you select?

- [1] Use Traditional IT - Acquire capital to cover maximum peak capacity expected
- [2] Use Hybrid Cloud - Acquire capital for average capacity. Use cloud services for peak demand
- [3] Use 100% Cloud - Relinquish physical server control and leverage a cloud with CRM services
- [4] No Idea

2. Assume you are an IT manager responsible for compliance with the Payment Card Industry (PCI) data security standard. Which option would you select?

- [1] Use Traditional IT - Acquire capital and software for credit card payment service
- [2] Use Hybrid Cloud - Connect business solution to cloud credit card payment service
- [3] Use 100% Cloud - Move business solution to a cloud with integrated PCI service
- [4] No Idea

The research offers a possible design depending on feedback from professionals and personal expertise about what could be affecting cloud risk views, and as such, the compromise decision process of implementing cloud processing. The conceptual design is depending on four vectors: (1) Skills and Knowledge; (2) Experience; (3) Cloud Perceptions; and, (4) attitude And Culture. The previews vectors are consider effecting the recognized threats accompanying with cloud

processing, and effect the tradeoffs between business advantages and security and complying conformity risks. Please refer to Figure 18 for the components constituting the tradeoff model between cloud business benefits and security and compliance risks. Notice that the skills and knowledge vector has two components that take into consideration abilities with both cloud computing and IT security. The Experience vector takes into consideration the years working on IT, period working with clouds, actual usage of cloud services, and the level of cloud adoption, which reflects the importance that cloud, has on the working environment of the participant. The Cloud Perceptions are measure based on two factors: the level of vulnerabilities associated with clouds, and the perceptions about the value of automation. The Attitude and Culture vector consist of two components: (1) individual attitude towards risk aversion reflected in the usage of social networking tools; and, (2) business culture, which consists of governance and innovation leadership

This research does not attempt to prove the conceptual model for cloud computing tradeoffs between benefits and risks described above, but instead offers this as a possible explanation of the observation, discussed later in section 8.1, that great disparities exist between cloud security experts and other IT professionals. The research focuses primarily on finding supporting evidence for the two main hypotheses, which are: (1) there are differences in risk perceptions between cloud security experts and other IT professionals; and, (2) deep knowledge of cloud security can have a conservative effect on the adoption of cloud services.

This survey was design to investigate opinions and perceptions of IT professionals toward cloud computing risks. The following eight risk parameters were included in the survey instrument:

1. Security risks perceptions
2. Regulatory Compliance risks perceptions Plus these Business Risks factors
3. Availability
4. Cost
5. Scalability

6. Flexibility and business agility
7. Control
8. Portability to clouds

3.4.2 Demographics – level of expertise

It is important to review the answers in the context of the level of expertise of the survey participants. We expected the answers to vary dramatically based on the level of cloud computing and security expertise. If a person works for a cloud provider, or their primary job is to secure or deploy a cloud service, the expectation is that this person will be more knowledgeable about cloud computing risks than others who are not working every day with cloud computing services. The basic hypothesis is that individuals with deep IT security skills and cloud computing experience will be well aware of security risks and compliance problems associated with cloud services, and will tend to be more conservative than those are unaware of cloud risks. Based on this hypothesis, there should be a correlation between expertise level and cloud risk awareness that is reflect in the risk tradeoff process between business benefits and security/compliance risks. The more experience a subject has, the more conscious and aware the person will be of cloud risks and cloud tradeoffs, and will reflect a conservative approach. To ensure understanding about the skill level of survey participants, we created skill categories. These categories were design based on subject classifications, which are valid partitions that account for the total population participating in the survey. Partition refers to groups of mutually exclusive subjects and the summation of partitions is exhaustive, embracing the entire population. Subject categories:

Expert: has done at least one cloud or security implementation.

Knowledgeable User: Has substantial use of cloud or security services but has not done an implementation.

Novice User: has limited use of cloud or security services.

Educated User: haven't used cloud/security services but understand the technologies

Unfamiliar User: has not used or implemented cloud/security services and is unaware of technologies supporting these services.

3.4.3 Cross-examination and rationalization of survey questions

In this section we review each of the survey questions to determine its relevance to this research and to help construct a better understanding about the perceptions of risks associated with cloud computing.

1- Demographics – level of skills

This question classifies the user across levels of expertise for cloud computing and security.

1. How would you rate your level of expertise on (1) cloud computing and (2) IT Security, where the expertise options are rank from high to low expertise?

1. **Expert** (have done at least one cloud/security implementation)
2. **Knowledgeable user** (substantial use of cloud/security services)
3. **Novice user** (limited use of cloud/security services)
4. **Educated** (haven't used cloud/security services but understand the technologies)
5. **Unfamiliar** (unaware of technologies)

2- Demographics – years of IT experience

The years of IT professional experience is part of the demographic information requested to identify the level of expertise, and adjust for possible generation gaps. Since this survey targets IT professionals, the expectation is to have very few

participants in the category of “No experience at all.” Participants with less than five years of IT professional experience are typically young professionals that are part of the Social Age generation (55).

Professionals with 5 to 25 years of experience are typically part of the Internet generation. The expectation is to have most of the participants be part of the Social Age and Internet generations. Some participants will have more than 25 years of IT professional experience and the expectation is that these will be approximately 40% of the participants.

2. How many years of IT professional experience do you have?

1. More than 25 years
2. 16 to 25 years
3. 5 to 15 years
4. Less than 5 years
5. No experience at all

3 – Demographics – Years of professional experience on Cloud Computing

The expectation is that the more time an individual spends using or designing cloud services, the more cloud expertise the individual is going to have. Level of expertise should be correlate to years of cloud experience. This demographic question helps establish expertise.

3. How many years of professional experience do you have using or designing cloud computing services?

1. More than 4 years

3 to 4 years

2. 1 to 2 years
3. Less than 1 year
4. No experience at all

4- What the deployment models of cloud you use?

In this Question it will help us to measure the most cloud deployment environment the experts are working with, what can give us mostly risky cloud area, Privet cloud These are typically owned by the respective enterprise and/or are leased. Functionalities are not directly expose to the customer, though, in some cases, services with cloud-enhanced features may be offered, which is similar to (Cloud) Software as a service from the customer's point of view, public cloud Enterprises may use cloud functionality from others, respectively, who offer their own services to users outside of the company. Providing the user with the actual capability to exploit the cloud features for his/her own purposes also allows other enterprises to outsource their services to such cloud providers, thus reducing costs and effort to build up their own infrastructure. As noted in the context of cloud types, the scope of functionalities thereby may differ. Hybrid cloud Hybrid clouds consist of a mixed employment of private and public cloud infrastructures, as to achieve a maximum of cost reduction through outsourcing while maintaining the desired degree of control over e.g. sensitive data by employing local private clouds. Community cloud typically, cloud systems are restricted to the local infrastructure - providers of public clouds offer their own infrastructure to customers (56)

4. What the deployment models of cloud you have using?

1. Privet cloud
2. Public cloud
3. Hybrid cloud
4. Community cloud

5 - Risk Assessment – Measure perception of risk on key risk vectors

This question attempts to measure the level of risk perceived by the subject. The list includes the top ten risk vectors associated with cloud computing implementations highlighted by the experts during the interview process. A Likert scale used to measure perceived increases and decreases about cloud risks compared to Traditional IT. Since our hypothesis is that there are differences in risk perceptions between cloud security experts and IT professionals, the expectation is that the following two aspects will be rank as “No Change in risk” or lower risk, which is different from the experts’ opinions.

- **Automation** - The average cloud user believes that automation is a vector that can minimize risks and improve an administrator’s efficiency. Unfortunately, as we discussed in Chapter2, automation failures can cause cloud storms, and this is a Key concern of some cloud experts interviewed for this research. We will review this risk vector under the Security Risks Framework and Business Risks Framework chapters.
- **Cloud Open Standards** - The average user does not see any new risks or advantages in new open standards, but the experts participating in this research see new APIs as possible alternatives to decrease cloud obscurity and empower cloud consumers to achieve automatic auditing of a cloud provider’s procedures. This vector can potentially lower cloud risks.

The rest of the technologies and trends are expect to be identify as “Moderately increases risk” or “Substantially increases risk.” The question helps answer the first two research questions related to the level of risks associated with cloud computing.

In addition, this question will help us build a pyramid of risk based on the opinions of IT professionals, and differences between this pyramid and the pyramid of risk built based on the experts’ interviews will help support the hypotheses that there are perception gaps between cloud security experts and IT professionals.

5. From the perspective of an IT provider, rate the level of IT risks associated with these cloud technologies and trends compared to Traditional IT.

Options ranked from High to Low risk:

1. substantially increases risk
2. moderately increases risk
3. No change in risk
4. moderately decreases risk
5. substantially decreases risk
6. I don't know

Options: 1, 2, 3, 4, 5, 6

1. Virtualization technologies (e.g., Hypervisors, virtualized networks)
2. Distributed Storage (e.g., Storage clouds, Files stored multiple times for Worldwide availability)
3. Distributed Databases (e.g. Eventually consistent databases, not SQL/Relational databases)
4. Authentication and Authorization (e.g., ACLs for billions of records)
5. Mega IT Data Centers (e.g., Consolidation of many data centers into gigantic cloud computing Data Centers)
6. Self-service IT Model (e.g., New single point of VM management)
7. Mobile Applications (e.g., Location-Based Range Queries)
8. Automation (e.g., scripts and interfaces for VM workflow automation)
9. Cloud open standards (e.g., OVF, OCCI)
10. Human Factors (e.g., human error, and insider threats)

6 - Framework – Prioritization

This question helps support the priorities addressed by the frameworks and by research question number three: “*What cloud computing characteristics are generating the most*

positive and negative impacts on security, business, and compliance risks?” This question also helps support assumptions about the value that clouds provide to customers.

6. From the perspective of a Cloud consumer, rate the importance of these cloud-computing services for your business.

Options are rank from very important to unimportant

1. Very Important
2. Important
3. Moderately Important
4. Of Little Importance
5. Unimportant
6. No Idea

Options: 1, 2, 3, 4, 5, 6

1. Reduce IT capital investment
2. Reduce cost of IT operations
3. Improve availability of application(s)
4. Provide flexibility to scale up during peak demand cycles
5. Support of mobile devices
6. Leverage cloud platform APIs to reduce development cost
7. Provide flexible payment schedule
8. Maintain high quality service to preserve reputation
9. Preserve security standards
10. Maintain Security Compliance certification

7 - Workload – Portability

The response to this exercise will help answer research question number six, “*What applications or solutions are appropriate to run on clouds?*”, and will help support the expert’s recommendations about workloads best suited for cloud computing. The experts explained that there seems to be a trend—the easier the application is to move to the cloud, the faster it would be adopted to cloud technology. In addition, the easier a workload is to move to cloud technology, the less opportunity there is for vendor lock-in since it can easily move to the next cloud vendor if there is dissatisfaction with the current cloud provider.

7. Rate the level of effort required to move these workloads to a cloud infrastructure.

Options are ranked from very difficult to very easy

1. Very Difficult
2. Difficult
3. Medium Difficulty
4. Easy
5. Very Easy
6. No Idea

Options: 1, 2, 3, 4, 5, 6

1. Social Networking Applications
2. e-commerce Applications
3. Data Analytics

4. Virtual Desktop
5. Development and Test workloads
6. Data Intensive Applications with residency/sovereignty compliance requirements
7. Healthcare applications with HIPAA compliance requirements
8. Legacy application
9. Banking Transactions Reconciliation Services
10. Customer Relationship Management (CRM)

8 – Cloud Perception – Perceptions about Cloud Vulnerabilities

This question helps answer research question one, “Are there any new security, business, and compliance risks associated with cloud computing technologies and *services*?” This question helps identify the perceptions about risks in cloud environments. The expectation is that most survey participants will select #2, identifying “some new vulnerabilities” on cloud environments, but experts believe the risk is too high for mission-critical applications with strong dependencies on compliance and security requirements.

8. Select the statement that best describes your thinking about cloud vulnerabilities.

1. Cloud can strongly support mission critical applications and doesn't create any new vulnerabilities
2. Cloud can support some mission critical applications but it creates some new vulnerabilities
3. Cloud is not ready for mission critical applications due to many new security vulnerabilities.
4. I don't know

9 - Cloud Perception - Perception about Automation Risks

This question helps quantify the level of perceived risk associated with automation. It helps answer the first two research questions since automation is a cloud-specific risk and as such does not exist in traditional IT. Experts believe that automation can bring risks to clouds in the form of “storms,” as described in Chapter 2, but most IT professionals that are not subject matter expert on cloud security do not seem to be aware of that risk.

9. Select the statement that best describes your thinking about cloud automation.

1. Cloud automation increases the effectiveness of system administrators
2. Cloud automation doesn't affect the effectiveness of system administrators
3. Cloud automation lowers the effectiveness of system administrators because it is complex technology
4. I don't know

10 – Cloud Risk Tradeoffs - Cloud security and compliance risks

This scenario attempts to test the perception of compliance risks in cloud environments. It creates a scenario in which the individual is required to make a tradeoff between the benefits of cloud adoption and possible additional compliance risks. The intent of this question is to determine the willingness of cloud adoption by IT professionals, in spite of compliance risks. Very common compliance risks with CRM solutions includes data locality. Due to lack of transparency from many cloud providers, the location of data sometimes cannot be assure.

The expectation is that IT professionals who are not subject matter experts on cloud security would think that 100 percent cloud is a good option, since SaaS solutions like Salesforce are popular in the US. However, businesses with data location requirements can experience penalties and even lose their business license if data locality requirements are not satisfied. A 100 percent clouds solution implies the usage of a storage cloud, which has many inherent security issues because of weak isolation of storage resources across customers in multitenant scenarios. The experts would advise the use of a Hybrid Cloud in these situations. The differences in cloud security perceptions between the experts and other IT professionals will help support the two hypotheses.

10. Assume you are an IT manager responsible for deploying a new Customer Relationship Management (CRM) solution. Which option would you select?

1. Use Traditional IT - Acquire capital to cover maximum peak capacity expected
2. Use Hybrid Cloud - Acquire capital for average capacity. Use cloud services for peak demand
3. Use 100% Cloud - Relinquish physical server control and leverage a cloud with CRM services
4. No Idea

11 – Cloud Risk Tradeoffs – Cloud security and compliance risks

This scenario attempts to test the perception of security and compliance risks in cloud environments. It creates a scenario in which the individual is required to make a tradeoff between cloud adoption, and additional risks associated with security and compliance. The intent of this question is to determine the willingness of IT professional to adopt cloud to minimize their work on PCI services, because they are

unaware of increased cloud security and compliance risks on sensitive transactions involving credit cards. The expectation is that IT professionals will select #2, to implement a hybrid cloud. However, the experts would advise the use of Traditional IT to control the end-to-end experience with payment transactions. The differences in cloud security perceptions between the experts and other IT professionals will help support the two hypotheses.

11. Assume you are an IT manager responsible for compliance with the Payment Card Industry (PCI) data security standard. Which option would you select?

5. Use Traditional IT - Acquire capital and software for credit card payment service
6. Use Hybrid Cloud - Connect business solution to cloud credit card payment service
7. Use 100% Cloud - Move business solution to a cloud with integrated PCI service
8. I don't know

12– Demographics - Cloud Experience: Level of Cloud Company adoption

The environment usually influences peoples' perceptions. This is why it is critical to understand the level of importance and adoption of cloud computing in the subject's company or immediate organization. The expectation is that the more important cloud is to an organization, the more cloud adoption a company has done and the more cloud expertise will be associated with the people who work for that organization. Level of cloud and security expertise should be correlated to the level of importance cloud has in the organization. This question helps establish demographics.

12. How important is cloud computing to your company?

1. **Very important** – Is one of the top priorities and currently fully enabling our business to use cloud computing.

2. **Important** – Is a significant goal and is currently enabling part of the business to use cloud computing.
3. **Medium Priority** – Is of average importance and some limited usage has taken place.
4. **Low Priority** – Is of little importance but there are plans to adopt this technology in the future.
5. **Not a Priority** – No plans to adopt cloud computing.

13 – Demographics - Attitude & Culture: Business Leadership in Innovation

The environment tends to influence peoples' attitude towards innovation and this could affect the willingness to take risks. This is why it critical to understand the level of importance, that innovation has on the subject's immediate organization. The expectation is that the more important innovation is to an organization, the more cloud adoption a company has done and the more cloud expertise will be associated with the people who work for that organization. Level of cloud and security expertise should be correlated to the level of importance innovation has in the organization. This question helps establish demographics.

13. How important is innovation to your company?

1. **Very important**-Is one of the top priorities and part of the culture to create better products and services.
2. **Important** – Is use as an important instrument to improve the business.
3. **Medium Priority** – Is of average importance and used to enable competing against rivals.
4. **Low Priority** – Is of little importance and sometimes driven by short-term opportunistic situations.
5. **Not a Priority** – Is NOT important to the business.

14 – Demographics - Attitude & Culture Vector: Business Leadership on Governance Approach

Business environments that value compliance could tend to influence peoples' attitude toward the need to maintain compliance. This is why it critical to understand the level of importance that compliance governance has on the subject's immediate organization. The expectation is that the more important compliance governance is to an organization, the more caution would be applied to cloud adoption. Level of compliance governance should be correlated to the level of importance innovation has in the organization. This question helps establish demographics.

14. How important is business governance, in support of regulatory compliance, to your company?

1. **Very important** – Is one of the top priorities and part of the culture to achieve high compliance.
2. **Important** – Is a significant instrument to achieve compliance
3. **Medium Priority** - Is of average importance to maintain normal industry compliance.
4. **Low Priority** – Is of little importance and followed to maintain minimum industry compliance.
5. **Not a Priority** – Is NOT important. The business operates on the edge of compliance.
- 6.

15 – Demographics - Expertise – Time spent on IaaS/PaaS

The expectation is that the more time an individual spends working with cloud services, the more cloud expertise the individual is going to have. Level of expertise should be correlate to the percentage of time of cloud usage. This demographic question helps establish expertise.

15. What percentage of your IT/computing usage is cloud based or uses cloud services like IaaS/PaaS (e.g., Amazon (AWS), Azure, Google apps, IBM Smart Cloud, etc.)?

1. More than 80%
2. 51% to 80%
3. 25% to 50%
4. Less than 25%
5. Don't use cloud services

16 – Demographics - Attitude & Culture Vector – Opinion on Social Networking sites

The anticipation is that the less information an individual has about protection, the more likely they are to invest some time on social networking sites. The level of security expertise should be inversely correlated to the percentage of time spent on social networking sites. The question helps to support the hypotheses about the role of risk perceptions since the IT professionals' defiance near social networking sites is different from that of the experts. Experts do not trust social networking sites, but the IT professionals are ready to take some chances in return for well connectivity. This demographic question helps establish expertise.

16. What best statement represents your opinion about Social Networking sites (e.g., Facebook, LinkedIn, and Google+)?

1. I do not know of any security issues associated with Social Networking sites. I believe these services provide a secure environment to connect with friends.
2. I am aware of some small security issues with Social Networking sites but I believe they do a reasonable job of protecting the privacy of their users.
3. I am aware of extensive security issues with Social Networking sites but I am willing to give up substantial personal privacy in return for social connectivity.

4. I do not use social networking tools because of extensive security issues.
5. I do not use social networking tools.

4. Research outcomes (risks resources of cloud technology)

4.1 *Highlighting*

In this area, we dissect the information to create useful information and draw out suggestions to IT professionals. The result of the information research is a selection of explanations that provide understanding about present cloud technology risks. Statements are base with cloud, data factors, and professional opinions. Moreover, the experts' ideas used to make a structure that could accomplish the assessment of Cloud threats and execution of minimization plans. The structure was enhanced using Delphi methods and is reinforce by the cloud expert's views. Very subjective grounding was the best possible way to support the structure suggestions since cloud is still very beginning in its adoption cycle. Available information is limited and inadequate to support extensive suggestions. The data was separate for two main categories:

- Factors that improve cloud risks.
- Factors that lower cloud risks.

This categories was designed to confirm the declare that cloud processing has new risks not existing in IT traditional, and as such, cloud risks are not the same as IT traditional risks. However, the results of this analysis display that there are many typical risks between IT traditional and the cloud, and that these risks cross, from Table 4. To demonstrate the declare that the set of cloud risks intersects with the set of conventional IT threats we offer a record of threat vectors that are distributed across the two sets and risk vectors that are exclusive to each set:

Table 4 risks between IT traditional and the cloud

IT traditional	Management of physical servers, laptops, management of physical firewalls, rigid hardware taxonomy, and upfront capital investment.
Cloud computing	Cloud image management, multitenancy, cloud automation scripts, and cloud management software.
In both	human factors, authentication, authorization, service level agreements (SLAs), Denial of Service attacks, and cryptography key management to just mention a few.

Source Author

The framework is distributed in the three main risks Sectors CSFR, CBFR and CCFR, the next parts review the findings, recommendations, and logic associate each risk Sector, and the way factors to contributing to the whole risk sectors affect clouds and their relative to traditionally IT, what can also The framework Presented within the perspective of (IaaS and PaaS), and some security situations are used to illustrate how to reduce risks.

4.2 Explanation of main cloud risks.

After comprehensive discussions and five parts of Delphi consensus building it became understandable that 12 main characteristics were typical issues among the questioned experts almost every cloud and security expert questioned described the four factors as

business and compliance risks and eight as security risks are which important. Most experts were eager to provide their justify opinions. During this part will present these Main risk factors and the next part ,Pyramid of Cloud computing security risks ,more specifics will be provided about the classification of the top 8 cloud computing security risk vectors compared to typical IT and how these touch the framework components. In the last few years clouds became most popular have gone from unknown to IT frenzy

4.2.1 Hypervisor Risks

This risk factor was cover extensively during the literature review and was one of the favorite topics of concern shared by experts interviewed for this research. The only experts who didn't agree with the risk to hypervisors were those with in-depth expertise on mainframe, and they insisted on equating mainframe logical partitions (LPARs) partitioning a physical machine into multiple logical partitions using the power chip architecture—as the “correct” way to do virtualization. Unfortunately, none of the cloud computing offerings available today use mainframe technology due to cost constraints; however, it could provide better isolation. For example, the IBM z10 mainframe based on the power chip design, which is very different from the commoditized Intel X86 microprocessor.

One of the advantages of the mainframe LPAR virtualization is that it has access to memory addresses that do not overlap. This eliminates the possibility of cross-VMs side-channel leakage risks typical of X86-commodity hardware. In addition, LPARs have separate registers for the hypervisor and the OS, which eliminates the risk of escaping the hypervisor during a buffer overflow (57) the risk associated with hypervisors can be easily reduced through more expensive alternatives like using extra-large VMs that consume the entire physical host, which eliminates most of the cross VM side channel leakages. The hypervisor reducing strategy requires a security/cost tradeoff. Users could implement a cloud with very good hypervisor isolation using LPARs, but this configuration could significantly exceed the cost of using extra-large VMs on commoditized hardware.

4.2.2 *Multitenancy*

Multitenancy, is resources are sharing the same infrastructure, as (memory, CPU, storage, firewalls, network switches, and other hardware components). multitenancy risk factor is related to those issues and associate with another case, that can be sharing with software of resource's, as (database, and backup services).

multitenancy cloud, is lead to sharing properties with competitors witch might engage in actions, that feat cross-VM isolation vulnerabilities, In this case an opponent could possibly acquire information about another organization, without the other organization learning the harmful activity.

In addition, if the customer has required by a court to offer data records and logs, into a multitenant there is a threat that some information on spread drives and commingled records might get to court from simple witness of VMS existing in same server.

4.2.3 *The new Attacks and Weakness.*

Cloud as new technology, is relative to new IT model that has a long maturity way, before became like now. The experts shared in this research some of these experts felt, that one of the risks was the unknown, from the time when the software and model have not being around lengthy enough to evaluate its risks in a measureable or statistical way. Day by day more enterprise customers trying or planning to move to cloud technology to accomplish greater success, Cloud technology is a collaboration of commoditized hardware and new software to given incarnations of old conceptions “hypervisors” as an example .

However, the business model:

1. Web services in a service-oriented architecture.
2. New automation technologies that created a perfect storm that enables cloud computing.
3. Pay by use.

However, this trend motivated the development, of many new programs as a service, and millions of users are not become consuming of clouds. With software that is not yet mature, No wonder we regularly read and hear about

security threats and conformity the process of cloud technology. from the advantage of cloud technology the new browser technology that what allowed plugins created for interface to use with new services, these browsers' additions tend to be many security vulnerabilities , as new software and application used by an IT we get the more new attack points.

4.2.4 Standardization & Automation

Standardization of cloud is the associated of risk with reducing the number of kinds of VMs available in the cloud. Standardization supports to make extra homogeneous location, but simultaneously this take down the barrier for distribute viruses or malicious software in clouds. Cloud gets his scales by mechanizing most of the information technology processes as the provisioning and deployment of new VMs, patch management, backups, load balancing, security monitoring, and others. Cloud computing SA (system administrators) manage many of servers through what called cloud dashboard and deploy processes with the push of a button. However, if a mistake made in the automation scripts this error can be replicate very quickly.

4.2.5 Authorization & Authentication

In the cloud, all the workloads/VMs are standardize to the lowest common denominator for IT processes. These might be better or worse that current company procedures. Some of the experts provided many examples to illustrate this problem. For example, Google App Engine supports OAuth (58) but the authentication only done against the Google Accounts service, creating the risk of duplicating identities between the enterprise LDAP and the Google service. In addition, to configure your Google App Web Application you need to create several XML (web.xml) files or YAML (app.yaml) files to define the way your application should run and the access privileges for it (45)This type of methodology is very coarse grained and doesn't support other business requirements like delegate authentication. Another example provided by the experts is Azure, which supports Secure Assertions Markup Language (SAML), and a Security Token Service (STS) to support this distributed identity management solution. The SAML protocol supports Single Sign-on (SSO), multiple authentication methods, and

minimizes duplication of identity between the enterprise customer and the cloud provider, but its adoption in the industry has been slow (59) .The main reason for the slow adoption has been interoperability issues when extending this solution beyond the intranet. We are still suffering from a proliferation of non-interoperable proprietary authentication and authorization solutions between cloud services that generate significant frustration for programs and security risks.

This risk factor is associated with the issues of handling a large number of users and data objects. How user identities verified in the cloud? How is access or privileges to services and resources granted in the cloud? Securely establish how can identity and privileges, past the many layers of services, in the cloud. Traditional identity and access management (IAM) technology that managed IDs and ACLs for 10,000 users, and the protection of a couple of million objects, simply does not work on the cloud scale of 200 million users and 100 billion files. IAM is predicate, on a centralized model that does not scale in a distributed environment like the cloud. The speed at which change requests to access controls occur in the cloud is much faster now than ever before and this creates more new challenges and risks. Several federated identity management systems and remote control authentication services have been create, but there is still no standard enterprise-grade tool across cloud services available today. The cloud business model that relies on a relatively easy access to IT resources makes it difficult to enforce rigorous authentication and authorization procedures.

4.2.6 Efficiency and Low Cost

Due to the current financial crisis, many businesses are experiencing great IT challenges, and are being ask to do more with less. This has encouraged more cloud adoption to leverage low cost IT for non-critical and non-confidential data. Clouds provide great efficiencies because they leverage the economies of scale of many thousands of servers and low cost of operations because of almost 100 percent automation. However, the low cost of the demand model has a hidden business risk, because it is a variable cost, depending on the workload. It is not always easy to predict

how much the total cost of operation will be for workloads that have unpredictable or unexpected peaks. However, with some understanding about how to calculate and estimate cloud capacity, this risk could be reduced and turned into a positive aspect of the business, allowing it to expand elastically with the cloud.

4.2.7 Legal Issues

An important business risk factor associated with clouds is how to negotiate and document service level agreements (SLA) as part of your cloud contract. SLAs need to be very well written and must include specifications for data management, location, and backups as well as accurate specifications to support audit procedures. Can the cloud provider guarantee appropriate disclosure and audit procedures but still maintain the privacy of clients sharing the cloud? Cloud providers must be able to explain how they ensure data privacy. Lack of specifications in an SLA can end up causing data privacy issues and even penalties. Likewise, cross-border issues are the responsibility of the business and not the cloud provider. The required location for compute resources and data storage should be specified

To avoid cross-border and data sovereignty issues.

4.2.8 Compliance and Cyber Forensics

This business risk factor is the most obvious one since everybody understands that there are penalties associated with failure to comply with government regulations. Compliance has been a hot topic for some time because in the last 13 years there has been a significant increase in regulatory compliance laws. This has posed significant challenges to traditional IT infrastructure, as well as to clouds. However, clouds are significantly more challenging by compliance processes because of the obscurity that some cloud providers maintain about their infrastructure processes. In addition, the transient nature of cloud consumption creates challenges about privacy and the auditability of logs. Sometimes cloud providers disallow cyber forensics or severely restrict the process. New regulatory compliance rules that require holding onto documents for a long period of time are also creating great pressure for the adoption of storage clouds that make it more affordable to comply with these regulations, but other risks increase if there is no control over storage and cyber forensics.

4.2.9 Concentration of Value

With the advent of mega IT data centers, many risks and challenges have emerged. Google and Amazon have documented the mega IT data center risks very well, and the experts interviewed for this research agree that cloud data centers are guaranteed to have a failure 100 percent of the time and to be under constant attack (60), (61). This means there will be a failure of storage or hosts somewhere in the cloud and thousands of attacks every day. Big centers are becoming big targets for elaborate new threats because of the big potential payout. This IT consolidation is creating value concentrations that are very attractive to malicious individuals and organized crime. This value concentration trend is not expected to change anytime soon, since the shift to consolidate into huge data centers is funded by cost reductions and energy efficiencies. The more value that is concentrated in the cloud, the bigger the target cloud services will become.

4.2.10 Endpoints

The emergence of mobile devices has put significant pressure on businesses to support interfaces with new endpoints. New mobile devices such as cell phones and tablets are part of mobile clouds and provide an enormous agility to employees. At the same time, these technologies open a large number of vulnerabilities to cloud solutions. For example, healthcare providers are under great pressure to support iPad applications to review medical records anywhere and anytime. This is a great challenge because many of the mobile devices are not complying with minimum-security standards and the software they use is still early in the maturity cycle.

4.2.11 Massive Amount of data accessible

The expectation and demand for data availability anytime and everywhere in the world has created an enormous challenge that sometimes is contrary to data consistency. New No-SQL distributed databases in the cloud have enabled great data availability at low cost, but at the price of lower consistency. Traditional relational SQL databases is tuned for accuracy and comply with the ACID (Atomicity Consistency Isolation Durability)

rule but they have lower data availability due to the locking mechanism of the two-phase commit. Many databases in cloud solutions will eventually follow consistent methods that optimize for availability instead of accuracy. Facebook is an example of a solution that uses an eventually consistent database technology. Massive amounts of data create challenges related to security risks associated with the capability to maintain data accuracy as well as minimize data loss and unauthorized access.

4.2.12 Human Factors

Insiders or system administrators' attacks are unfortunately still one of the top concerns of the experts interviewed for this research. However, this should not surprise us since it is still one of the key concerns about traditional IT (62) as well. Our experts explained how cloud providers have gone through extensive efforts to install sophisticated monitoring tools on the administrator's console and dashboard terminals. These tools monitor changes made by system administrators, in the hopes of discouraging malicious or disgruntled employees who might steal information or sabotage the system. However, this particular risk factor is expected to continue to be a problem for the near future since the more technology programmers create and throw at this problem to reduce technical vulnerabilities, the more emphasis attackers give to the human element. According to Kevin Mitnik (63) one of the world's most famous hackers, breaking the "human firewall" is easy. In addition, more than 70 percent of the experts interviewed for this research cautioned about the danger of social-engineered attacks that exploit people's vulnerabilities, and the way attacks targeted at cloud administrators could cause insiders to unintentionally enable malicious intruders.

4.3 Framework risks of cloud computing

From , discussed with the experts their thoughts about the most risky cloud computing risk vectors, , but it was not until the modified Delphi rounds of consensus making that we first accumulated insight on the ranking in the top higher 8 cloud computing risks compared to traditional IT. Several of cloud computing security events are not disclose, most cloud-computing providers will not state their own weaknesses, making it

difficult to quantify the security risk factors in cloud environments. For that reason, this finding about the top eight cloud risk vectors and their ranking based on increased risk compared to traditional IT is of particular importance. Experts interviewed provided great value in enabling a qualitative view of these security risks. To illustrate the relative importance of these eight cloud security risks, during one of the Delphi consensus building rounds one of the experts suggested building a pyramid to illustrate the ranking of the top eight cloud risk vectors. After the Delphi participants gained agreement about the ranking order of the top eight cloud risks, a diagram created using a pyramid paradigm. The bottom of the pyramid represents the highest risk vector and the top of the pyramid is the lowest risk vector. The diagram sent to the four experts to gain validation on the ranking and the pyramid paradigm to illustrate the relative risks compared to traditional IT. The final version of the agreed-to and validated of cloud risks is show in Figure 18, which includes a brief explanation on each of the risk vectors in a side box.

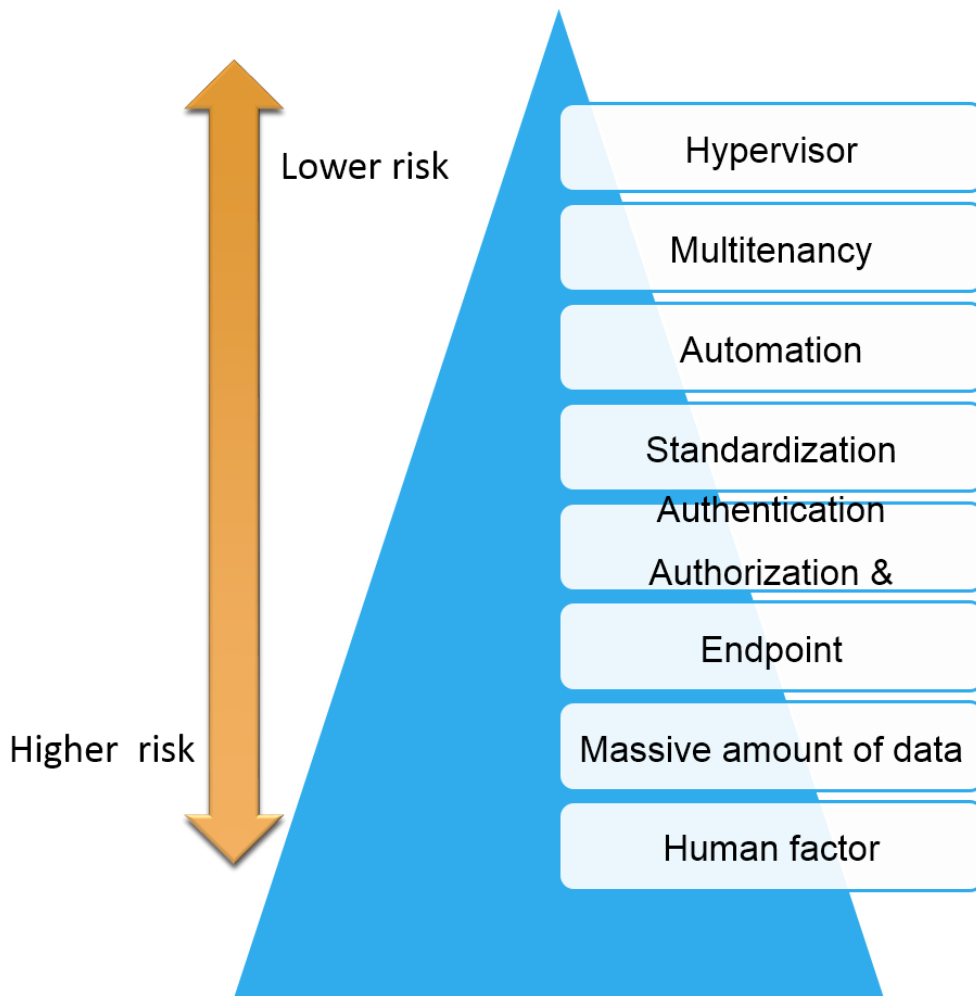
4.4 Cloud risks pyramid bases on experts

During the one-on-one interviews, we discussed with the experts their opinions about the most dangerous cloud risk vectors, but it was not until the modified Delphi rounds of consensus building that we first gained insight on the ranking of the top eight cloud risks compared to traditional IT. Many cloud security events not disclosed and most cloud providers will not admit their own weaknesses, making it difficult to quantify the security risk factors in cloud environments.

For that reason, this finding about the top eight cloud risk vectors and their ranking based on increased risk compared to traditional IT is of particular importance. The tacit knowledge and insight provided by the experts interviewed provided great value in enabling a qualitative view of these security risks. To illustrate the relative importance of these eight cloud security risks, during one of the Delphi consensus building rounds one of the experts suggested building a pyramid to illustrate the ranking of the top eight cloud risk vectors. After the Delphi participants gained agreement about the ranking order of the top eight cloud risks, a diagram created using a pyramid paradigm. The

bottom of the pyramid represents the highest risk vector and the top of the pyramid is the lowest risk vector. The diagram was sent to all 4 experts to gain validation on the ranking and the pyramid paradigm to illustrate the relative risks compared to traditional IT. The final version of the agreed-to and validated pyramid of cloud risks illustrated in Figure 18 Cloud Risks Based on Experts”.

Figure 18 Cloud Risks Based on Experts



5. Discussion and interviews result

5.1 *Cloud security risks framework (CSRF)*

The purpose of the Cloud Risks Framework is primarily to answer two questions:

1. What criteria should be use when evaluating a cloud provider?
2. What can done to reduce risks associated with cloud solutions?

This framework is intended to answer the “what” not the “how” about cloud risks. Cloud computing is in its infancy and technology supporting this new IT model is changing very quickly. Therefore the answers to “how” are too transient to be addressed by this research. Instead, we will focus on more fundamental aspects of cloud risk that will persist for some time, even as new technologies emerge to reduce some of these risks. The task of evaluating cloud solutions for the purpose of selecting an IaaS or PaaS can be immensely simplified when we know what to look for.

The data provided in this section is the result of a qualitative analysis from four interviews with cloud and security experts. As a result, this section focuses on the experiences and insights provided by these experts and does not attempt to answer quantitative risk measurements or specific implementations. In addition, the reducing recommendations in this chapter and discussed extensively during the modified Delphi rounds of consensus building. However, the recommendations were neither statistically confirmed no validated on their effectiveness and the reader should not conclude that these are the only possible reducing strategies for the cloud risk vectors. Additional research should done to validate and quantify the effectiveness of the reducing strategies offered by this research.

In this section, we are going to focus on the vectors that increase security risks in clouds, and the process and methodology to evaluate and reduce those risks. The data provided in this section was generate through the evaluation and qualitative analysis of security risks provided by security and cloud experts who generously shared their understanding and insight about how to improve security exposures in cloud environments. This section uses the CSRF diagram

Table 5 to describe the concepts and factors associated with security risks in cloud environments, and provides systematic details about what a cloud user should look for to reduce their security risks. To facilitate the understanding of the cloud risks, each risk vector was assigned an arrow that depicts the risk associated with cloud compared to traditional IT. The arrows on the CSRFs as well as the business and compliance frameworks were assigned based on the votes received from the experts using the calibration spreadsheet tool.

Table 5 Cloud Security Risks Framework

The new Attacks and Weakness	
1. Cloud Management	
Cloud administration software	▲
Automation scripts	▲
Portal & APIs interfaces	▲
2. Virtual servers	
Modern Hypervisors are as big as operating systems which creates significant attack surface	▲
VM images	▲
hypervisor vulnerabilities	▲
cross VM leakage via side channels	▲
3. Virtual storage	
file system	▲
long-term storage management	▲
database partition management	▲
4. Virtual networks	
virtual network switches	▲
virtual firewalls	▲
Network protection software for virtual networks	▲
DNS services to map virtual network to internet IP address	▲
5. Multitenancy and standardization	
Complexity	▲
Few standard VMs Lower It Configuration Diversification	▲
Competitors share IT resources	▲
6. Authentication and authorization	
Authentication bridges between cloud layers and services	▲
orders of magnitude increase on users requiring authentication	▲
identity federation	▲
7. Endpoint	
mobile device vulnerabilities	▲

browsers as the primary interface to clouds vulnerable plugins	Red
Security	
Value Concentration	
more transactions than prior IT data centers	Red
Human Factors and insider attacks	Red
Mega data center	Orange
physical security of mega data centers	Green
cloud providers have more IT skills	Green
More Data	
Cryptography key management	Red
Data Privacy on shared resources	Red
data on usage patterns	Red
cloud users contact information	Red
Multi petabytes of data backups and Redundancy	Red
data services optimized for availability and partition tolerant	Orange

- The green mark: Expresses lower aggregated risk associated with cloud for the risk vector when compared to traditional IT.
- The red mark: Expresses higher aggregated risk associated with cloud for the risk vector when compared to traditional IT.
- The Orange mark: Expresses no change in risk between cloud and traditional IT for the risk vector.

The framework of cloud computing security was divide to the 3 main concepts:

1. additional attack surface
2. more data
3. value concentration

5.1.1 Authorization & Authentication Factors.

To verify the identity of users, cloud computing providers use the Authentication, lightweight directory access protocol or (LDAP), is the convenient way to traditional IT to set all information for fast access requires, through private secure network, the

issue of the cloud computing is the require the recurrently updated, where the traditional IT Technique will not be solution for cloud, while cloud services running over unsecure networks “internet”, right now cloud providers offers some kind services in support of their cloud services, google App an example (64), google app can offer authentication service only with their account service, which give this method limited and then makes google apps attractive for big customers, Authentications is based on knowns things as (password, ID.PIN, fingerprint, voice, eye geometry, etc..) where can divide them to typical authentication ID, Password, which user knowledge what is less secure, also cloud need to support single sign on (SSO) what make authenticate through the many cloud services layers more easy .

Cloud computing doesn't have strong authentication methodology, that what our experts was noted, Authorization os very close to Authentication works from side what kind of data and resources can user access to, OAuth is standard makes authorization process more secure and effective in clouds .

5.1.1.1 Reducing Strategy for Authorization and Authentication.

- Distributed Authentication

To avoid the risk of getting locked into a single cloud proprietary authentication service and duplicating identities, it is best to use a distributed authentication service that can easily authenticate separate services without having to log on again. A service like Kerberos is ideal for cloud authentication; however, it still not embraced widely across cloud providers.

- Use Strong Distributed Authentication and Authorization services

When possible do not use proprietary services from cloud providers that are not well federated or do not support a distributed architecture. These proprietary services can generate duplicate IDs from the authentication/authorization systems and the cloud services. If possible, use strong and distributed authentication services like Kerberos and distributed authorization services like OAuth.

- Multi-factor Authentication

Avoid single factor authentication services because these easily to spoofed. Some cloud providers have started to provide multi factor authentication as part of their configuration options. It is very important for configurations updated to ensure services support multi-factor Authentication.

- Use Challenge-Response tests

To lower the likelihood that malicious users will be successful in automating the creation of new user IDs, a challenge-response program like should be used, which requires human intervention to analyze and produce a viable response. The intention of using a challenge response test is to be able to distinguish between a computer and a human. This process does not guarantee the intentions of the person, but it will at least ensure that it is a human and not a machine.

- Remove Inactive or Suspicious users

Test the validity of users through data analytics, and evaluate the outliers. If a user has unusual behavior, investigate the source and conduct of this user. If it warrants suspension of services, create a process you can use to quarantine the user or terminate the ID. This is where frequent monitoring of users pays off, by eliminating possible sources of attacks.

5.1.2 Cloud computing Administration Factor

The software and services of cloud administration connected management stack of cloud where is the significant amount of code is necessary for administration software

and services of cloud the what will found new attack Surfaces that can be broken for mean purposes.

Also from other point the ripeness of cloud management software comparable low and this inevitably seems to be weaknesses reason, also programming interfaces the typically based over Web Services to connect cloud services as IBM Smart Cloud ,Amazon, Google App .etc....

In the flowing part, we will review some of the Advices that got from the experts through the interview, where not all of them are agree with it but that the advantage of using a Delphi method which helps to increase understanding from experts in parts of this investigation where is not much documentation and data case of cloud computing.

That advices not being measure on how they reducing cloud risks but given a map and explanation on how some of the cloud attacks can be reduce.

5.1.2.1 Reducing Strategy for Cloud Administration

From the interview method was clear that one of the main point with cloud computing services is that numbers of cloud users keep follow their cloud provider advices, following the guidance and advices of cloud providers is the safety and easy way To reduce the risk related to cloud administration software what we was noted in the previous section (23) different and same cloud technique not always can be applied to another clouds. Meaning that, cloud provider should use his own managing service which allowed all that work perfectly, that also can be solve by another vender solution day to day cloud computing getting more clients and establish more cloud services his managing services f cloud can be stranded which can be in soon future known, so the cloud provider responsibilities including standard configurations verified by the seller. The tasks made by the cloud buyer are consequently reduced.

- **Data Backups**

One of important and the traditional Data security is backups and disaster recovery, aim of this solution that keeping data system be recovery by using different cloud provider mean at less cannot be only with the same cloud provider.

- **Automation and cloud administration software**

Within previous section we had spoken about new attack surface which has created by automation and cloud administration software which the factor has been out the user control, the best way to keep it safe that stay as separated as possible from the particulars of the cloud provider's APIs, which enabling simple activity of a remedy to other cloud when necessary. Automation and cloud administration can be reduced by creating penalties in the service level agreement (SLAs)

- **Isolation Layer**

With isolation layer will create a levels of abstraction between the cloud client and cloud provider application program interface (APIs) This abstraction has the prospective to reduce source lock-in and helps the migration to another cloud provider in case any problem happened.

5.1.3 Virtualization Factor

Virtualization that enables us to partitioning one server to multiple servers ((simulation)) that simulation can be open the cloud to many topics such as insufficient isolation, factor risk of Virtualization has more than one type

1. virtual networks
2. virtual storage
3. virtual servers

So in this section we would like to make Virtualization risk factor more clear for the IT manger, from other way that we already stated the concern that virtualization added a more attack surface for the cloud computing, so a one of Example, can pointedly

reduce this type of risk VMware is working to take out the Linux based service console, to reduce their hypervisor footprint from 2GB to 100MB (65) that reduction in footprint lessens the risk related with this attack surface. Sprawling of VMs. is another type of experience that often common since hypervisors easier the process of making new VM examples, so to solve some of that problem most IT's creating VMs as a replacement of reconfiguring old method, but don't difficulty to take away resources are not needed, If the cloud doesn't have a good process to verify patches and force updates on inactive VMs, these can quickly get out of date and become not only a honeycomb for viruses, but also a drag on performance.

Virtualization technology also facilitates the process of capturing VM images, which significantly increases security risks on two fronts. First, the convenience of VM image creation facilitates the sharing of VMs. At the same time, malware and perhaps confidential information can also be unintentionally shared if appropriate filters or protection is not in place.in next section describes and end-to-end solutions to manage VM image in a secure way.

The second aspect that image capturing creates is the representation of the virtual system in a file. If the file is not encrypted it can easily be read by anyone who gains access to the disk where the file resides. On traditional systems the running operating system uses the BIOS (basic I/O services) interfaces to write the data stack to ROM (read only memory), maintain status information, and process the executable. In a virtualized environment the hypervisor simulates the BIOS interfaces. Instead of using ROM, it writes to a file on disk, which is the VM image. If the image file is not encrypted and a malicious individual gains access to the disk where the VM image is resident, all the information in the VM will be accessible to the intruder, even if the VM is at rest Hypervisor not only virtualizes the host memory and CPU, but also the storage available for the VMs. The size and type of storage provided depends on the type of VM selected.

The typical VM configuration comes with ephemeral storage. This type of storage is transient and only available when the VM is active. It is destroyed after the VM instance

is deleted. Ephemeral storage is also referred to as local storage, and can be equated to your local disk in your PC. However, in cloud configurations it can't be assumed that the ephemeral storage is indeed local, since it is most likely in remote storage shared across multiple VMs. If highly confidential information is kept on ephemeral storage, there is a risk that a malicious attack can escape the hypervisor and gain access to the confidential data, which is located on storage that is usually shared by other VMs in the same host. Most applications running on VMs also require long-term storage, which is where databases or other information are kept between VMs instantiations. If the long-term storage is not encrypted, other users may inadvertently or intentionally gain access to sensitive data

5.1.3.1 Reducing Strategy for Virtualization

Minimize Hypervisor footprint – To reduce the risk associated with an additional attack surface, select a Type 1 hypervisor with minimum footprint. Type 2 hypervisor tend to be significantly bigger as we reviewed in Chapter 2. The experts explained that the smaller the code associated with the hypervisor and the closer it is to the firmware the less risk associated with the additional surface space.

1. **To clean often** – Avoid sprawling of VMs by removing frequently inactive VMs this can be achieved by reminding users to delete their VMs or enforcing time limitations on inactive VMs. In either case, to avoid security exposures, inactive VMs should continue to be patched until they are removed. Also, old accounts that haven't been used in a while should be removed to avoid hackers using those accounts for malicious exploits. Also, a company-wide process should be established to name VMs and rename VMs that don't comply. This will avoid future problems as the numbers of VMs and VM images grow in the future.
2. **Do Patch Often** – Since hypervisors are still going through a sharp maturity curve it is important to stay current with patches and upgrade to the latest version as soon as possible. This advice also applies to virtual networks since a

vulnerability on your virtual network can expose your entire virtualized system. The concept “patch often” also applies to the virtual network components.

3. **Off risky Hypervisor commands** – Reduce the risk of hypervisors by disabling or limiting the use of commands or tools most frequently used by hackers to break into a virtualized environment. Some of these tools use private communication channels between the hypervisor and the host OS that allows cross VM communication. For example, the tools VMchat, VMcat, VMftp use the ComChannel in VMWare to gain access across VMs. Follow the configuration recommendations provided by the hypervisor vendor since a well-configured virtualized environment will be more difficult to break. In 2011, VMware provided a report about how to configure their hypervisor. This guide should be followed by anyone thinking about using VMware (66).
4. **Avoid Sharing Host** – In the case of VMs that need a secure location, a multitenant environment should be avoided, and a private cloud should be used instead. If budget constraints preclude the use of a private cloud, extra-large VMs that utilize the entire physical host can be selected, which essentially avoids sharing the host with others. This kind of workaround is quite effective for mitigating most of the multitenancy risks.
5. **Monitor VMs** – One of the advantages of virtualized images is the ability to do VM introspection. This introspection capability can be used to monitor VMs and analyze the volume of data, behavior, and traffic going through VMs to identify outlier situations, which can help defend against critical problems.
6. **Separate network traffic by security profile** – VMs with similar security Profiles should be grouped together, and each group’s network traffic isolated by assigning them to different VLAN ports. Also, to ensure the administrator has access to VMs during an attack, like DoS, the management network traffic

should be isolated from the rest of the VM traffic. Refer to Figure 22 for network architecture.

7. **Private storage** – An excellent way to reduce the risk of storing sensitive data in virtualized environments is to use private or dedicated storage for this kind of information. However, this option is sometimes too costly. The more reasonable alternative is to encrypt data that has high privacy requirements.
8. **Encrypt important data** – It is difficult to isolate data on shared storage and the best protection available against intruders is to encrypt sensitive data.
9. **Make save Storage zones** – If a business has high security requirements on data like PHI (personal health information), it is best to negotiate a private or dedicated long-term storage with the cloud provider to ensure privacy. Also, private storage should be encrypted and protected by firewalls.
10. **Make save your virtual network** – Several layers of switches and firewalls should be created around the network to have multiple barriers against intruders. Use protection software for virtual networks. Disable DNS services that can help map virtual addresses to intruders. Keep virtual firewalls and virtual switches software updated.
11. **Subdivision Sensitive Data** – Put additional protection around your most sensitive data and confidential information. For example, establish a secure zone for long-term storage that is encrypted and not accessible by administrators without prior authorization. Also, network traffic should be segmented based on secure profiles since the network needs to be as secure as the data it transport
12. **Achieve Security Audits** – Make sure growth procedures finish frequent protection audits on web programs to prevent the most common strikes, such as

SQL-injection and cross-site-encrypting. Other way, frequent third celebration audits should be recognized to acquire a neutral viewpoint about security preparedness.

13. **Safe Storage Processes** – Understand how ephemeral storage space is recycled across VMs to ensure no data is shared inadvertently. Also, it is important to know the method used to dispose of long term storage space volumes, to confirm that no confidential data remains kept in storage space after the volumes are decommissioned. Also, data should be partitioned based on security requirements, and separate long-term “secure zone” storage used for sensitive data. Encrypt that data using your own key management system.

5.1.4 Multitenancy & Standardization Factors

Capability of sharing hardware resource and software service through multiple users running independent workloads is call **Multitenancy**. A multitenant environment is usually characterize by a service instance that is share across many users, and it is the responsibility of the service to maintain isolation across the multiple tenants. Multitenant solutions are design for transient usage, and separate the tenant’s data based on the security policy established for the service. However, problems sometime arise due to lack of isolation between tenants caused by a hypervisor’s vulnerabilities, or weaknesses in the software supporting the service. Due to multitenancy and virtualization, a dangerous situation that can happen is to have two competitors sharing the same physical host. If data requires high levels of privacy, it is best not to share a physical host with other users in a multitenant environment like a cloud, because of the many vulnerabilities of hypervisors. However, sometimes the consumer of cloud services is using Software as a Service (SaaS) and does not have an alternative—or the interfaces—to isolate his data. Examples of SaaS solutions are Facebook, Windows Live, and Salesforce.com, where users share under the covers of the website databases containing the tenants’ data The risk of a third party having access to your data is real, either inadvertently, due to a mistake or software malfunction, or maliciously, through exploitation of vulnerabilities and malware. Unfortunately, this occurs more frequently than most users and vendors are willing to advertise. The best way to verify the level

of security in a multitenant, environment is by testing the security and proving it is secure. You can test the level of security you need by performing an audit on the service and by using an ethical hacker to attempt to penetrate your service. If your ethical hacker is able to penetrate the solution, it means that others can do the same. Multitenant solutions are relative immature, so until security is tested to comply with a particular security requirement, you cannot be sure that it is compliant with that requirement. It is also important with multitenant solutions to ask about backups, archives, and recoveries. Can administrators access data without requesting your permission? Can you encrypt your sensitive data and manage your own encryption keys? It is important to understand how the tenants' data is archived, or the services provider, to ensure that each tenant's data can be retrieved separately, creates backups. This process ensures that information is not advertently provided to the wrong user. For example, in the case of a (SaaS) customer getting a court subpoena, if that customer has archived data was commingled with yours, you do not want your archived data to be sent to court or to a third party for review without your authorization. Another risk factor to keep in mind is the standardization processes that clouds create. Standardization is generally is a good thing for most businesses because it simplifies support and encourages reuse. However, when every image in a cloud is a standard image, a malicious intruder will encounter fewer barriers to spreading attacks because of the low diversity of configurations on VMs. The combination of standardization and multitenancy also creates a double exposure because the security of the system will only be as strong as the weakest link. In this case, the weakest link tends to be high-risk images shared by high-risk tenants.

5.1.4.1 Reducing Strategy for Multitenancy and Standardization.

1. Segregation of VMs by security profile

Group VMs with similar security profiles to ensure VMs with the most stringent security requirements are host together. This helps the system administrator focus on monitoring the most critical VMs through automatic procedures, as well as by

manual inspection. A good way to group VMs is by using VLAN ports for different levels of security profiles, as discussed in prior section

2. Avoid Shared Resources

For businesses with high confidentiality and integrity requirements for their data, it is best to avoid multitenancy environments. However, due to cost this is sometimes an unrealistic goal. The next best alternative is to limit the amount of sharing your usage pattern or solution has with others. For example, if you are using a cloud at the PaaS or IaaS level, you can use extra-large VMs to avoid sharing the physical server with others since most extra large VMs utilize dedicated physical hosts. If you are at the SaaS level, you can negotiate with your service provider, to create for you a separate instance of the data service. Another, more expensive alternative could be to use private storage in combination with the SaaS service, to store your data at your traditional IT data center or outsourcing provider.

3. Penetration test

Because of the complexity created by multitenancy, and the risks associated with failing to keep tenants' data confidential, many experts interviewed strongly recommended that regular penetration tests be performed. These kinds of tests can help establish a more realistic assessment of the risks associated with the cloud service.

4. Test early, well and often

It is well understood in the industry that the more you test your software the better quality you will have. However, the need to test automation scripts cannot be stressed enough. Because of the risk of exposing a significant amount of customer data, it is imperative to test automation scripts very well and regression test every time they are updated. Because some scenarios can only be tested with high stress or volumes on the system, it is best to dedicate a significant amount of time to stress testing.

5. Desynchronize Disk IO activities

Automation has many advantages, but also a few disadvantages. As customers consume standard images they tend to follow the exact procedures defined by the original image. This can create a wave of VMs attempting to do virus protection or disk utility scans all at the same time. To avoid this kind of unnecessary synchronization, and wave of IO activity, it is best to create a function that updates the scheduled times to ensure different execution times for scanning activities like antivirus protection and check disk utilities. This can be achieved through an additional step after the image installation, to ensure the IO-intensive activities are staggered to minimize impact on the overall system performance.

6. Change Management Process

Since clouds change very fast—especially multitenant SaaS applications—it is very important for cloud providers and tenants to establish a well-documented change management process. This process ensures a transition that migrates tenants gradually to newer versions of the software.

7. Establish an Audit Process

If a multitenant service cannot be audited, it should not be used. Establishing transparency between the cloud provider and the tenants is very important. An audit process can help create transparency and help consumers understand how their data is handled. The audit process must include virtual networks, host systems, data storage, databases, administrative procedures, and third party software used by the multitenant solution provider.

8. Data Encryption

Encrypting your data is a mitigation strategy shared with virtualization and other risks factors, in situations where data integrity and confidentiality is in jeopardy.

5.2 *Cloud business risks framework (CBRF)*

In this, part we going talk about CBRF and its purpose is to guide IT managers and decision makers regarding what to look for and things to consider when making a business decision about cloud. The Business Risks Framework reviews and illustrates the five most important business factors mentioned by the experts who participated in this research. The simulations and calculations provided within this framework are small illustrations about how to evaluate cloud availability and costs. We advise IT professionals to avoid get caught up in the particulars of the examples but instead focus on the approach. It is expected that modifications will be required to simulate and calculate the cost of a particular commercial situation since every IT installation is different. The five risk factors covered under the Business Risks Factors are Cost, Efficiency, Control, Availability, and Legal Complexity. Each of these factors is described below, with a detailed explanation about why they are important to cloud and to security experts an analysis of some contrarian views is included as well. Each factor is followed with a reducing strategy that can assist IT managers in coping with the uncertainties of IT transformation and the business decision of adopting cloud technology.

5.2.1 *Legal Problem*

Greatest typical cloud computing contracts are centered on (as is) warranties an example of those problems include not clear and restrictive laws, lack of precedents to guide litigation, and frequent trans-border operations, (as is) mean that the provider of cloud services doesn't promises of any kind that mean no clear guarantee will be prospered or that it will meet the customer's expectations, not all cloud service provider afford SLAs (Service-level agreement) And that what will determine the guarantees Usually it will be on the basis of limited commitment and availability, This is measured through the gate cloud uptime, rather than the actual reliability of customer service and performance,there is also the lack of standards is other problem for cloud contracts because there is no uniform way of providing cloud services and there are no uniform standards to help measure the quality of service. And those that determine the guarantees.

In addition, when cloud service and customer are located in different countries and data is resident in multiple countries so the Trans-border data flows are common problem, and that came from creating costly litigation fees because of unclear and contradictory law, because the Data flow that crosses a country's borders is subject to the jurisdiction of multiple countries.

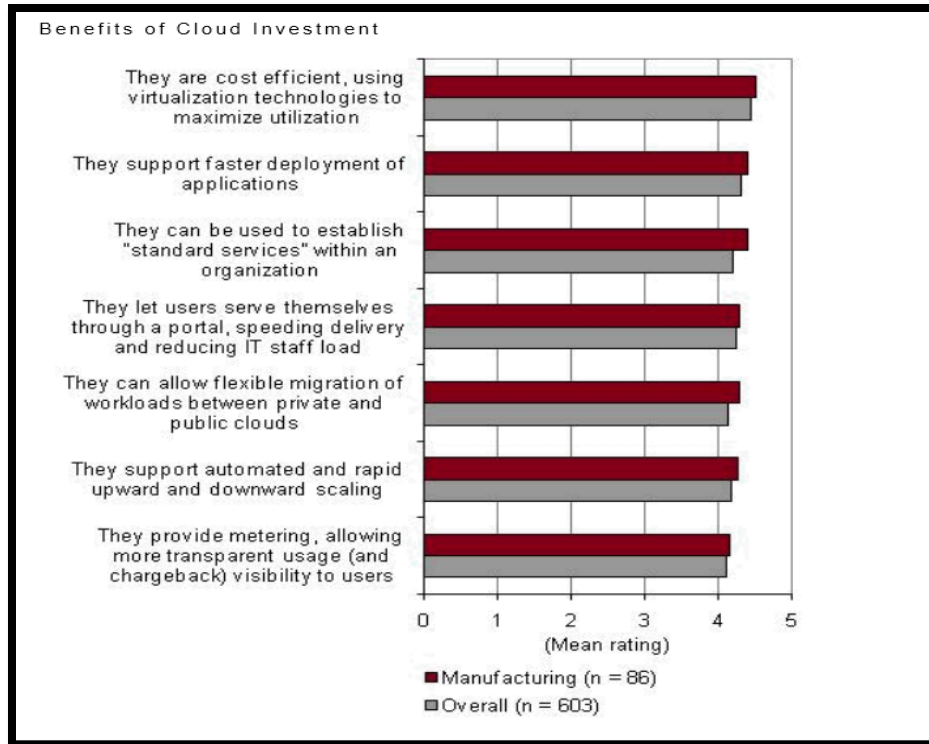
From those legal issues and the disparities between IT regulations depending on country may will get case of a dispute so here can be question, under which law country is this should handle the dispute.

So related to this case or another the contract negotiating processing must include specifications of the Data location at all times, security and performance assurances, and country jurisdiction and litigation processing in the event of a dispute, from other point the contract should be designed in way that encourages the desired conduct to reducing contract risks. But still the best written contract can be facing by risks related with unclear laws, an example, it is not clear if customers or cloud providers ((own inference data, data derived from other data, made through the usage of cloud services)), also no intellectual property regarding in clouds, data in clouds protected by intellectual capital laws? What protection exists if data infringed, Should the IT professionals explore country rules and mandates regarding data retention, location, and disposal?

5.2.2 Efficiency

One of the main reasons for shift to cloud is the cost which saving money expenditure and operational expenses, according to the IDC Manufacturing Insights: IT Strategies report by Bob Parker the survey has shown 2nd most important reason to Shift to cloud which Support faster deployment of applications (67) , for creating a data center it may take so long time, what is need the obtain capital approval also so this period called “lead time” including configure systems, purchase hardware, and deploy a solution.

Figure 19 Benefits of Cloud Investment



Source: (67)

Provides as many VMs as needed within a few minutes needed on another hand. What gave significant improvements in agility and efficiency to the business, Clouds has improve automated with APIs and web services that allowed users to added automate their own workloads to make more agility and to simple complex tasks, “Workflows for scaling workloads on demand” is an example of automation .Cloud can helps running VM for a many hours at the same level of complexity as hundred VMs for one hour and also in same price, mean that cloud can run workload more faster than traditional IT, mean you pay cost of one amount and you get 2 time faster what allowed you processing for tow, an example image calculations performed by Pixar Animation Studios because every frame rendering take eight hours to render by one processor host, in simple explanation single Pentium III ProLiant server working 24/7 for 278 days. With the URS, the rendering of The Painter only took three months to render (68) elasticity that large dynamic resources bring to the cloud Scalability. The scalability of clouds because of their natural elasticity is one of them aspects that reduce cloud risks

related with efficiency, cost, and availability, worldwide IT resources that can empower medium and small businesses to leverage opportunities in other areas of the world.

Enormous efficiencies for clouds can be created by automation and Standardization through substantial reduction in configuration choices and also there is some of Disadvantages to standardization and automation, software levels available in the cloud, standardization limits the number of operating systems.

5.2.2.1 Reducing Strategy for Efficiency

1. Reconfigure and redesign of cloud computing

Moving workloads “as is” sometimes is not the most effective way to utilized cloud resources. For a workload to achieve the maximum economic benefit and scale horizontally automatically, it needs to be redesigned with cloud scaling in mind. If you have a monolithic application, it could be beneficial to divide the workload into smaller executable components that can take advantage of the cloud elasticity. Also, workloads need to be adjusted to interface with the cloud APIs and web services to automatically instantiate VMs when required, delete unnecessary resources to avoid needless charges, and achieve an effective load balance across VMs. Without effective configuration and adoption of the cloud provider APIs and services for optimization, solutions won’t run as efficiently as possible.

2. Use the right tool for your workload

Each cloud solutions has different IT requirements and it is important to use the right tool for the job. Many cloud solutions use new programming languages like Python, PHP, and Ruby on Rails. These types of programming and scripting languages require management and development tools designed to be used with them, and extensions that facilitate the usage of cloud APIs and services. Some examples of new tools are Freedom OS (provider of tools to develop and manage workloads based on JBoss and JPaaS) and Zend (tools to mange PHP workloads).

3. Optimize your cloud solution

There are many cloud management tools that are able to monitor and optimize workloads hosted on virtual environments, and that can greatly facilitate the management of VMs. Cloud elasticity is fantastic at providing the capacity necessary on demand, but keep in mind that the requests for additional resources should be managed to optimize your business and not necessarily the IT service. This means we might want to delay a calculation or service if it could cost less at a later time or be done on a smaller VM without affecting the potential income. The balance between business needs and IT optimization can be achieved using some of the new cloud management tools like xCAT (open source distributed computing management tool), Scalr (a collection of site management tools than can help manage loads on Amazon, Rackspace, and other cloud providers), and RightScale, which was designed specifically for the cloud architecture.

4. Create a Disaster Recovery Plan

It is out of your control to prevent “cloud storms,” and since sooner or later there will be some type of unfortunate mistake that could affect your solutions, it is best to prepare for a disaster. If host instances run in the same data center, moving to a cloud cannot be considered a disaster recovery plan. A disaster recovery plan should include data centers from multiple cloud providers. However, if a single cloud provider is used, a minimum configuration should include two data centers in different locations, with significant network redundancy, including at least two different network suppliers. Keep in mind that more resources within the same cloud won’t mitigate the risk of a “cloud storm” produced by a mistake in an automation script. Clouds provide good availability, but still can’t be assured 100 percent, and business solutions running on clouds still need a disaster recovery plan.

5. Patch Often

To mitigate the lack of diversity of operating systems and middleware versions and types, it is recommended that users and cloud providers follow a process to continuously update software to the latest level. Stay informed on vulnerability reports

and make sure your cloud provider uses the latest operating system versions and patches

5.2.3 Availability

Hardware failure or called "downtime due" in cloud computing is different than Traditional IT, because the Question how server can be recover faster from that failure, in cloud computing to recover Failures event it can be more easy than traditional IT may take few minutes within automatic scripts and instantiation of VMs, which explaining behave very differently than traditional IT which takes few days or week to recover from backups ,but still should note that cloud more common failure than traditional IT, so the cloud providers should provide services to automate the recovery process help reduce the recovery time to only a couple of Minutes.

Because of massive numbers of storage and systems running at mega data centers, could computing be more failure than traditional IT, in “Reasons for Cloud Application Failure” (69) Chris Preimesberger mention nine reasons for cloud failures, but how those can be reduced?

5.2.3.1 Reducing Strategy for Availability:

1. Calculate Availability

It is important to understand the current availability as well as the possible future availability with new IT configurations. Measure MTTF in the traditional IT data center before moving to the cloud. Construct a realistic view about the current probability of system failure and overall availability. When moving to the cloud, include in the SLAs the availability expected, and dedicate a budget to automate the recovery process. After the service is in the cloud, test the availability by stressing the service. Simulate a DoS attack to ensure the solution will work correctly when an actual DoS attack happens.

2. Document Availability Requirements

In order to assess the availability risks and do an analysis of business tradeoffs between cost and downtime, IT managers need to understand the availability requirements of

the business. If IT managers don't understand the availability requirements, they might spend too much money keeping availability that doesn't provide any additional financial benefit. Also, misunderstanding availability requirements can generate an under-investment in automation and resources, which can result in significant downtime that affects the business's reputation. It is important to align business requirements for availability with the IT strategy and planning process to avoid gaps that can negatively affect the business

3. Automate Recovery Process

To benefit from higher availability in the clouds an investment must be made in automating the recovery process. Moving a workload to a cloud without investing in automating the recovery process would not provide any availability benefits, and could in some instances provide inferior availability

4. Monitor for outliers

Be proactive in defending against DoS attacks. If request loads are substantially higher than expected, consult your cloud provider to validate network activity and the origin of possible attacks. Cloud providers constantly monitor the network volumes for possible DoS attacks and can help block attacks coming from external servers, or within the same cloud.

5. Create a Disaster Recovery Plan

This recommendation has been mentioned in several of the risk factors because the cloud experts who participated in this research stressed that this is one of the biggest misconceptions of cloud consumers. Clouds do not protect against catastrophic events and it is necessary to build a solid disaster recovery plan using data centers in different locations, with plenty of redundancy.

5.2.4 *Controller*

Lack of transparency was maintain from our experts as one of disadvantages, where the cloud provider should take it in mind to power the trust with customers, from the expert point of view that more details and the guarantees described within Service-level agreement (SLA) from the cloud provider it can enhance confidence, contract can protect user when there is lack of services, but not when there is lock-in risks, code specific APIs for cloud provider should be Isolated that what can reduce the Lock-in risk and what user can take it seriously, by APIs user can easy shift to another cloud provider if there is problem with current provider. With the traditonal IT the IT workers normal controlling their Resources, However, they should take new method of managing Through the (IaaS) level or (Paas) level instead the physical level, what gives good availability in low cost, ask about the benefits of cloud move its must important point what the experts focus on , what the benefits will get our clients with services hosted on cloud ? What the financial cost? In addition, how fast business grow can cloud provide? From the interviews was so clear that the experts could tell the difference between IT risks and business benefits.

5.2.4.1 Reducing Strategy for Control.

1. Educate IT Managers

If IT managers understand the reasons and business benefits for moving to the cloud, less pushback and resistance can be expected from IT personnel

2. Create Clear Contractual Agreements

If you plan to run a considerable amount of work in the cloud, it is advisable to create a contract or SLA stating your expectations and requirements. Don't accept the standard contract you get on the web when you first register with a credit card. Those contracts are written for the benefit of cloud providers, and usually include indemnification clauses. It is standard practice to create contracts with cloud providers

not only to ensure service and compliance procedures, but also to allow the cloud provider to make any updates necessary for your workload.

3. Control by the Numbers

The control points on IaaS and PaaS moves from the physical layer to the VM layer. Appropriate cloud tools should be utilized to ensure cloud services are optimized for your business needs. Also, monitoring the workload can help measure the actual versus expected benefits, to ensure the project remains on target and doesn't end up over budget. The more data you collect, the better analysis you can make and more control you can exert on the utilization of the VMs.

4. Create Isolation Layer

Avoid cloud lock-in by keeping customization related to cloud APIs and automation scripts encapsulated in a few modules to facilitate movement to other clouds if necessary.

5. Demand Transparency

Do not let a cloud provider claim "security by obscurity," because as a consumer of IT resources you must know how your data and workloads will be managed. To mitigate this concern, request inspection of the physical data center facility, and audit the IT processes associated with your workloads before signing a long-term contract with the cloud provider

5.2.5 Costing

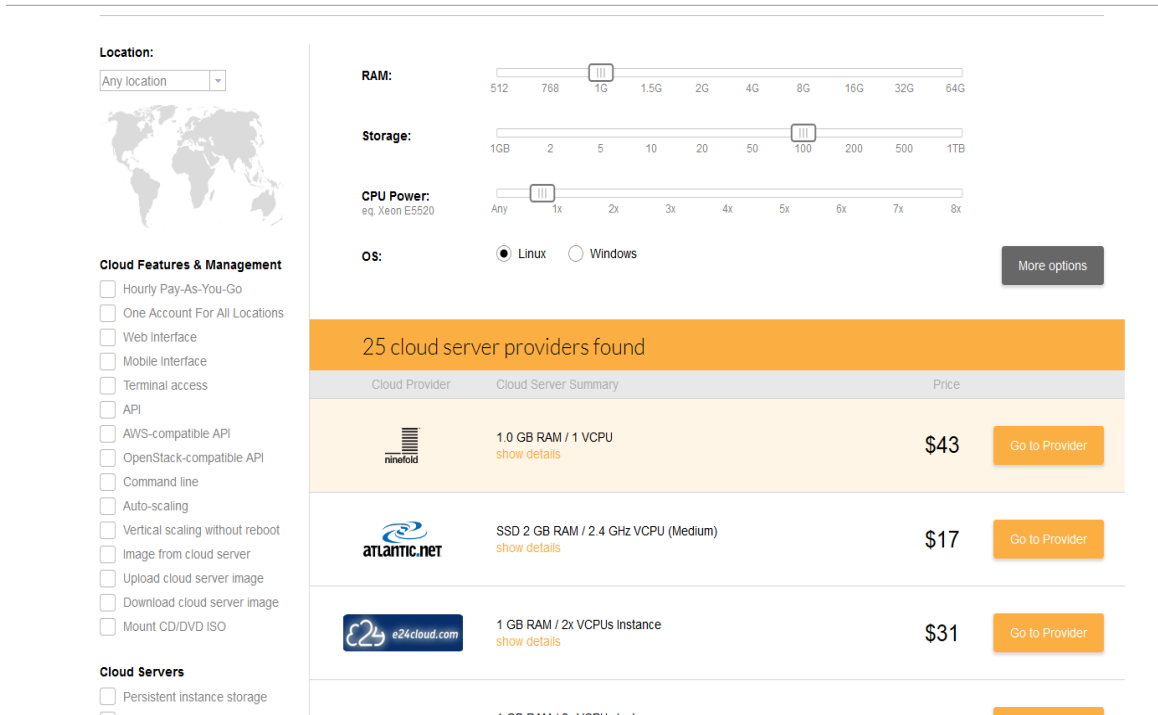
During the interview most of the expert agree that cost is one of the important factors, which effect on bossiness risks,

Reducing operational cost and provides amount of payment as you pay only as what u consume. Since the training required and skills to maintain VMs is lower than what is need it for traditional IT ,in this point not only the experts were focusing in but also many other research as well (70) (71) (72),

Still the Question if that pricing flexibility reducing business risks? In addition, why is there so much confusion about the cost of the cloud? It may because all the clouds are different. So why there is no standard of price VMs today? Meaning “measurement to price VMs”, an example electricity It is easy to compare pricing because all the electric companies use the same unit of measurement.

Some clouds using RAM as unit of measurement like “GoGird” but another using CPU as units etc... , so how we estimate the cloud cost? so the fast way that we use the possible tools what offerd by the cloud provider to cost estimate that will be the first way , and than we can comparing that with an other servers what we get from another cloud provider , where the price it will be the first options of that compration in case they have same benifet , from the expert point of view that is not necessary because the many source cloud calculators already available or we use price comparison engine like Clouddorado (73) which allowed us to calculate many cases with gaven price per hour automatically depaned on our configuration selected Figure 20

Figure 20 Cloud Server Comparison



Source: www.cloudorado.com 2014

As next step of comparing cost of VMs evaluate the overall cost related with cloud which are currently placed in data center .

(MIPS) or of infrastructures per second usually the computer cost measured ,where most of the IT systems is little when we compared with hardware cost , electricity, operations , and software has become more significant, that what make cloud more economical which reduces the labor cost and builds in front of traditional IT in cost .

Table 6 Advantage of cloud VS Traditional IT in Cost

key cost	Cloud Competing	Traditional IT
Buying Power	discounts are significant	discounts are not provide
Power	cloud mega data centers located in low electricity area	Cannot be different than business center
Operations and Labor Cost	heavily automated, one operator is able to handle thousands of computers	one system administrator is usually responsible for 150
Commoditized Hardware	built with “white boxes”	assembled with parts provided with not independent vendors
High utilization	choose from many workloads to maintain their systems	lack of virtualization, no multitenancy, and a small number of instances works

5.2.5.1 Reducing Strategy for Cost

To Shift to cloud computing is long-term transformation business, outsources etc.. From Additional IT staff which expensive for the corporation who thinking move to cloud in begging, this plan must be perform deeply and clearly on the risks of cost when the making finally decision here some point what expert are advising who’s going to shift to cloud :

1. **Calculate your current cost**
2. **Estimate Cloud Migration Cost**
3. **Compare Cloud Providers**
4. **Leverage Spot Instances**
5. **Automate To achieve the lowest possible cost in clouds**
6. **Compare current IT versus Cloud**

5.3 *Cloud compliance risks framework (CCRF)*

The newest economic problems is an example of activities that have introduced more regulation and government intervention to businesses. New rules have been designed to facilitate auditability, secure customers, and to force businesses to follow tight bookkeeping and confirming procedures. Cloud and security experts interviewed for this research expressed deep concerns and issues with clouds, and their ability to satisfy regulatory compliance. The professionals playing this research known to compliance as “the process of satisfying the requirements of the business.” This process included government regulations, commercial demands, and specific business procedures. Government regulatory compliance includes regulations like the Sarbanes-Oxley Act of 2002 (SOX), which established new audit standards to increase business transparency and ethical behavior. Another example of a new regulatory compliance law is the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), enacted in 2010. This legislation is not restricted to financial institutions. It affects business government, business reports, and professional settlement. There are many industry-specific conformity rules such as FFIEC, HIPAA, and ISO 2700 X, NIST, PCI, and others. The task is to make an IT support that can guarantee the procedure of sticking to regulating, commercial, and business techniques to get the preferred conformity stage. In the same time, this IT service should happen without duplication of effort or excessive complexity, and of course, at an affordable cost. This research spent a significant amount of time with experts, investigating the source of risks associated with compliance on cloud environments. This chapter focuses on describing the findings of the analysis and additional specifically the vectors that have an effect on the compliance risk issue, during this analysis of compliance, we have a tendency to center on the vectors associated with restrictive and business compliance, We acknowledge the importance of business specific or structure compliance. but since those needs modification from company to company, less stress was placed on risk vectors poignant those needs. Future analysis ought to assess a lot of closely the variations between risk vectors poignant restrictive and industrial compliance versus structure compliance, Out of these vectors, seven area unit thought of to extend the

risks of compliance on cloud environments in comparison with ancient IT. Allow us to review every of those vectors very well and discuss why specialists known them as vectors which will probably increase the danger of not achieving compliance.

5.3.1 Data Retention

This is the sole compliance risk vector that the specialists thought of to be lower risk in clouds than in ancient IT, The supply of the cloud advantage is that the low storage value obtainable from most cloud suppliers. Cloud customers will simply store their information multiple times , and for a protracted amount of your time, at a fraction of the price of a traditional IT, Also, by default several cloud suppliers copy information files many times (e.g., 3 times).

to extend the information accessibility on artefact hardware, as a byproduct this copy method will increase information retention. the rise of knowledge retention comes at the price of problems relating to information removal and remnants, Substantial compliance problems will be created by several copies of data files on obscured data storage, with no accessible APIs to validate removal, but at a similar time this method is what will increase Data retention within the clouds, The overall accord of the specialists was that data retention could be a risk vector that has lower risk within the clouds than in traditional IT.

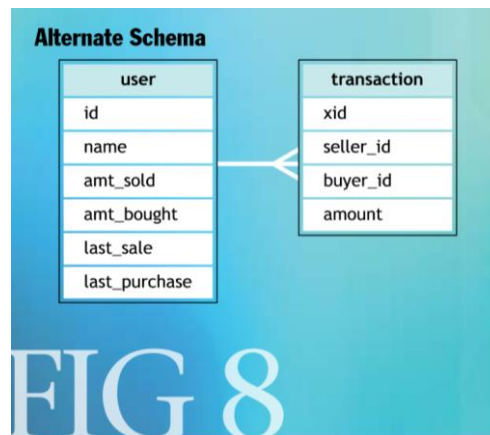
5.3.2 Data integrity

This risk vector received several divergent views and supporting factors, A few consultants considered it a high-risk vector in situations related to solutions that need high data integrity and consistency, in same time most of the workloads that presently run on clouds, a substantial range of specialists felt it number overall risks, through many discussion and driving accord among the experts through a Delphi method. The conclusion was that this risk vector is neutral. Its positive and negative effects on compliance can rely upon the standard of data services enforced within the cloud.

Some of the specialists expressed the chance of integrity as a byproduct of upper risk for data segmentation, other experts pointed to cloud advantages like lower storage cost, which inspires frequent automatic data backups and reduces the time to recover

from potential data integrity problems , also there is other experts pointed to the newest styles in data design and management, where the data are often classified by the level of integrity needed, and differing kinds of management systems and lockup mechanisms which will be applied to suit the requirements of the various data sets, mean the cloud data management service ought to be architected supported the data integrity requirements of the required resolution, and for data that needs constant integrity and any lapse in consistency will produce important issues, there is strategies to spot this sort of sensitive data and build special ACID rules for it that only locks a tiny low section of data set to assist deal with cloud data partitioning risks (74)

Figure 21 Alternative Schema



Source: An Acid Alternative by Dan Pritchett, Ebay 2014

Finally, the experts decided the three are a number of risks as well as a number of benefits, of running big data sets within the clouds, and that the aggregate risk of data integrity remains unaffected if a high quality data service is implemented within the cloud.

5.3.3 *Data segmentation*

From the environments of cloud computing, where the access of data is possible from anywhere by any time, there is many benefits came from distribution of multi data what's mean that data sources is out of service and also create good capacity for access and performance, here by Segmentation of data we get new risk that increased probability encountering transmission failures crosswise data repositories, what called

((data consistency)), the way how data stored in traditional IT is different than Cloud Data Stored , we have explained previews part Data integrity look . In cloud Data segmentation risks are very high, but with technological engineering and the use of appropriate data can reducing those risks rules.

5.3.4 Data Remnants and removal

Nowadays it is important to be ensure the secure removal of data, (MSP) which providers and managed service provider, customer of cloud computing would incur audit risks, still the Compliance responsibilities related to the enterprises who using cloud quite than with Provider. cloud provider can be unsuccessful with procedures of the SLAs, and cloud customer can also not be unsuccessful with compliance as a result of the vendor's execution of requested procedures, where the provider don't cover the customers for compliance penalties, any financial responsibility is sustained by the business (Users) not by the provider.

5.3.5 Data Access

Cloud computing has generally a large number of users, and looking after accurate access for vast sums of millions of users, through the research appendage, many of the experts interviewed portrayed deep issues about dangers associated with data accession in swarm environments, Some providers of cloud get better operations for approach management as compared to others.

but in the mass data accessibility tends to be perceived by experts as some of weakness associated with clouds. There are numerous protocols for authentication and authorization utilized by cloud providers, Included in this are SAML, OAuth, OpenID, and many more we mentioned within the CSRFpart, it is the dynamic nature of clouds that poses difficult to assuring accurate data access in a manner that is audit-friendly, and that includes audit trails to put up with strong security demands required by lots of new laws and regulations.

More than one of providers can support access control lists (ACLs) delivered by customers, but as being the constant change of access controls accelerates, lack of

interfaces to enable distributed access management rules can pose risk, because of supports a distributed architecture OAuth is attractive, and between cloud providers and the customer IT environments has possibility of eliminates duplication of access controls, from other side currently OAuth doesn't support multi factor authentication found in other services.

In addition, there may be another weakness risks that originated the lack of cloud application programming interface (APIs), to allow the management of logs linked to access controls, that what gives cloud customers power to control and audit their cloud data access, by negotiating with all the provider to offer access controls to the customers, or creating some kind of interface, what will be reducing that risk

5.3.6 Lack of Standard Cloud certification process

The cloud technology is the evolution of the traditional IT, is necessary to note that some of the practices that used for traditional IT, can be used to cloud technology, But still lacking some of the certifications and the specific practices, CSA or Cloud Security Alliance, (75) has done for cloud computing implementations a security guidance, where is no certification for providers of cloud, to be following appropriate policies and procedures for cloud computing, to have an agency or free cloud authority (non-cloud provider), dedicated to independently check clouds for specific worries, as overall cloud security, that what the expert was agreed with by interviewed, in same time some of them are go to cloud agency verify cloud services for more trust of cloud providers, this kind of independent agency can make clouds more trusty for the customers.

5.3.7 Reducing Strategy for Compliance

5.3.7.1 The Agreement.

Within (SLA) compliance requirements should be describes, even specific organizational required processes, clear negotiated agreement with the provider, the clear gaining and maintaining regulatory compliance for the IT managers can get.

5.3.7.2 Arbitration.

As documented as the communication structure and Arbitration can be power full to achieving compliance, Arbitration can be intersection of industry regulations, regulatory laws, and technology, the experts was agree that the Arbitron is important force to driving the processes, that achieve compliance not the other way, to reduce m what is commercial ,governing, and business compliance wants to force by an IT organization, Also the responsibility and roles is very important to avoid conflict, from other way the business compliance targets can be affects if the choices about who will modifying the arbitration, and that what the expert was agree with another literature (45)

5.3.7.3 APIs.

Data removal and remnants is problem, one of many Issues what the experts were focus, as data locality, where the APIs is the easy way to reduce that problem, by activate automatic audit and verification, as example for solve that, on the cloud storage can be build GPS location services and create APIs that will verified data area, that will power trust of consumer, and cloud compliance risks.

5.3.7.4 Images Control.

Self-service process, one of the cloud unique characteristics, which allowed users to makes, his own Network configurations, VMs, and images that can be businesses advantage, what gives speed to react to unexpected demand and agility, so in case the cloud images not controlled and maintained, can generate many compliance problems, the cloud experts' advice to build governance to cloud images creation, to be sure is more quality, and standardization,

5.3.7.5 Support for Cyber Forensics

There is some risks can be connect with compliance penalties, an example court subpoenas and legal ramifications, what drives to design plan support cyber forensics, an ethical hacker can help somehow, by design the strategy what can be written in SLA contracts, those main keys cloud images, hardware configuration, access control change requests, Retention of data such as logs, Retention of data such as logs.

5.3.7.6 The independence of the cloud certificate

The experts note to reduce the risks of governmental and regulatory of compliance, increase the qualified of compliance evaluations and independent auditors to perform security, and publish the results, also classification system for clouds, is another experts mention, what allowed the customer of cloud to identified cloud provider quality, which gives the IT manger knowledge about Quality of the provider, before going forward with using his services.

5.3.7.7 Automation.

By the survey result, more than 70% of professionals, IT decided that automation increases the effectiveness of system administration, the advantage of cloud computing over traditional IT in automation tools is so clear because automation enables clouds to scale massively, and help maintain scraps to automate most IT works.

6. Survey results and recommendations

With this part we are going to give more details about the survey result, from of the experts and Professional IT point of view, also we are going to base on some other outcomes may it will be helpful for the IT manager. Also some of recommendations what our surveyors are provide for cloud adoption, also including this recommendation will be advices for the some warnings must be taken when shift to cloud.

6.1 Survey results

6.1.1 Demographics

To verify the expertise level of the participants, this survey was designed with many questions related to demographics. The survey questions and their relationship to the main research questions and hypothesis were explained in Chapter 3, where we covered the methodology conducted by this investigation. The projected level of expertise of the survey participants was to obtain 58 % or more of the candidates in the category of Knowledgeable User and Novice User. The expected number of participants in the category of Experts was approximately 20 percent. A cross-examination of the expertise level responses with other demographic questions, such as years of IT experience, years working on cloud implementations, and percentage of time using cloud services, indicated that many participants who identified themselves as experts were not really experts. For example, some of the survey participants who identified themselves as experts only had two years or less of experience designing clouds, and their usage of cloud services was below 50 percent of their total IT usage. To consider a survey participant a true expert, with skills equivalent to the experts who participated in the interviews, the individual must satisfy these minimum requirements:

1. Select “Expert” for cloud skills in question #1.
2. Select “Expert” for security in question #1.
3. Fifty percent or more of the IT time usage dedicated to cloud services in question #15.
4. Fifteen years or more of IT experience in question # 3.
5. Four years or more of cloud design experience in question # 4.

Unfortunately, only four of the 101 survey participants satisfied all these requirements. This means that only four of the participants were Experts. The survey demographics reflect that the skill level of Knowledgeable held by 58 % of the population, and “Novice” by another 17 % of the population. On the lower end of the skill spectrum, 20 % were “Educated” and 1 % were “Unfamiliar.” Table 5 shows the skill levels of the participants adjusted with the demographic data to reflect a more accurate picture of the actual skill levels of survey participants.

Table 7 Skill levels of survey participants adjusted with demographic data

Level	User	Percentage
Educated	20	20%
Experts	4	4%
Knowledgeable	59	58%
Novice	17	17%
Unfamiliar	1	1%
Total	101	100%

In table 6 illustrates the self-selected level of expertise of survey participants, which is a substantial over-estimation of actual skills, based on the demographic data, and not close to the four percent (4 people) of the survey, participants who can actually considered “Experts.”

Table 8 Skill levels selected by survey participants

Level	Percentage
Educated	20%
Experts	26%
Knowledgeable	43%
Novice	26%
Unfamiliar	1%
Total	100%

The survey found that only 40 % of the survey participants spent more than 25 % of their time working on cloud services, more surprising was to learn that 12% of the participants had not spent any time at all using clouds Table 7.

Table 9 Professional experience designing cloud services

Experience	Percentage
More than 4 years	21.8
3 to 4 years	25.2
1 to 2 years	26.7
Less than 1 year	8.9
No experience at all	0

However, although a substantial number of cloud security experts did not participate in the survey, the level of overall IT expertise was good. As a result, the survey provided insights on the cloud risks perceptions of IT professional who are not necessarily subject matter experts.

Table 10 Years of IT professional experience

Experience	Percentage
More than 25 years	42.1
16 to 25 years	33.2
5 to 15 years	21.8
Less than 5 years	1
No experience at all	0

The following table illustrate the results of the demographic questions.

Table 11 Percentage of IT usage based on cloud services

Using	Percentage
More than 80%	7.3
51% to 80%	15
25% to 50%	18
Less than 25%	48
Don't use cloud services	12.1

6.1.2 Cloud Vulnerabilities

This survey helped investigate and gain insight about the perception of IT professionals regarding cloud risks, and possible new vulnerabilities that cloud technologies bring to

the table that didn't exist before in traditional IT. Our analysis shows an over whelming 74% of participants stated that cloud computing can support some mission-critical workloads, but that it creates some new vulnerabilities. This strong response from the survey participants provides supporting evidence that a large percentage of IT professionals perceive and think of cloud services as creating new vulnerabilities. In addition, this strong response, as illustrated in table 10 helps support the claim that cloud risks are perceived as new and unique IT risks.

Table 12 Perceptions about cloud vulnerabilities

Cloud vulnerabilities.	Percentages
Cloud can strongly support mission critical applications and doesn't create any new vulnerabilities	5.8%
Cloud can support some mission critical applications but it creates some new vulnerabilities	74.1%
Cloud is not ready for mission critical applications due to many new security vulnerabilities	20.1%
I don't know	0%

To make evaluation by IT professionals' a Likert scale was used for cloud risk perceptions compared to traditional IT. The risk vectors used by the Likert scale question were the top risks identified by the experts during the interviews and illustrated as a pyramid as part of the outcome from the Delphi iterations. The outcome of the survey are illustrated in Table 13.

Table 13 Survey participants' risk perceptions about cloud vectors

option	substantially increases risk	moderately increases risk	No change in risk	moderately decreases risk	substantially decreases risk	I don't know
1. Virtualization technologies	30%	27%	19%	9%	13%	2%
2. Distributed Storage	36%	31%	8%	9%	6%	2%
3. Distributed Databases	31%	29%	20%	6%	4%	10%
4. Authentication and Authorization	29%	27%	23%	7%	5%	9%
5. Mega IT Data Centers	28%	34%	18%	8%	11%	1%
6. Self-service IT Model	27%	31%	22%	7%	9%	4%
7. Mobile Applications	30%	33%	19%	7%	5%	6%
8. Automation	21%	17%	32%	13%	10%	7%
9. Cloud open standards	11%	9%	38%	17%	14%	11%
10. Human Factors	29%	34%	22%	6%	5%	4%

Where the risk vectors rank are based on how they increase the overall cloud risk compared to traditional IT. The risks were count adding the survey votes assigned to the Likert scale categories of “Substantially Increases Risk” and “Moderately Increases Risk.” This joint value was the number used to establish the ranking of cloud risk vectors compared to traditional IT. In addition, responses to this survey question enabled the creation of a cloud risk pyramid, Based on the data provided by 101 IT

professionals. Table 12 illustrates the way cloud risks compare to traditional IT when ranked by IT professionals who are not subject matter experts on cloud security. The ranking of the risk vectors in Table 13 is the same order used to build the pyramid of risks based on the survey data.

By cloud computing risks Pyramid, hypervisor as risks, estimated by using the term of virtualization within the survey mean these risks was ended because virtualization to IT professionals is common concept than hypervisor where is more technical.

6.1.3 Other Correlations

This research has get strong connection between advancement and the significance of cloud to businesses According to the information, 85 % of members believe advancement is essential or very essential for their organization. Concerning cloud technology importance, 76.7 % of members claimed cloud is to be important or very important to the business. Based on this data, if a business values the importance of cloud, it is 100 % likely the business also values innovation. The reverse relationship has only 90 percent correlation. This means that if a business values innovation, it is 90 percent likely that it values cloud. However, if we focus only on those who responded “very important,” we see the gap widening on the correlation between the importance of innovation and cloud, with an 80 % correlation. According to this information, this indicates some founders are in sectors that are not quite prepared for cloud, due to present threat stages Guidance for Cloud Computing Adoption

In addition, we found great connection between the significance of advancement to a company and powerful significance regarding regulating conformity. This is not an amazing finding since high levels of advancement are required to fulfill complicated conformity specifications. In addition, with the fast speed of change in regulating conformity, a modern business cloud is need to ensure sticking to regularly evolving

6.2 Recommendations for cloud computing adoption

The adoption of cloud computing is a topic of great interest to IT director and IT professionals who are looking for ways to improve their services and value to the corporation. However, what value do IT professionals hope to obtain from cloud computing? What cloud characteristics or services are of most importance to cloud consumers? It is important to understand what IT professionals are looking for by adopting cloud services. This understanding enables appropriate guidance regarding cloud adoption, to ensure alignment of the desires of IT professionals with the capabilities of cloud technology. Based on the Survey data, we have supporting evidence about what 101 IT professionals value most from cloud computing. As we discussed in Chapter 3, this data was obtain using a Likert scale and the ranking of the cloud services was done based on the importance of the cloud services to cloud consumers. The importance was quantified adding the survey votes assigned to the Likert scale categories of “Very Important” and “Important.” This joint value was the amount use to establish the order of importance for the cloud services by this research and is illustrate Based on this survey data and input from the experts, we can assert with confidence that Customers are looking for the following top six cloud benefits.

1. Improve availability of applications. This translates to fast recovery if a VM fails.
2. Reduce cost of IT operations.
3. Maintain high quality service to preserve reputation.
4. Flexibility to scale up during peak demand. This means provisioning of multiple VMs over peak demand periods to ensure the quality and availability of the service.
5. Preserve security standards.
6. Reduce IT capital investment.

From the preceding list, built from the survey data obtained by this research, we can see that most cloud customers are motivated by the potential cloud financial benefits that could bring lower cost of operations, no capital investment, and flexible IT.

However, IT professionals in general, based on the experts' opinions and survey data; still do not want to give up security. This presents a tradeoff between security and financial benefits. As we reviewed before, in the cloud security risks framework, cloud environments can create, significant new risks compared to traditional IT. The desire to preserve security standards can present many challenges in the cloud

6.3 *Other outcomes*

We found very good supporting evidence that IT professionals with not much experience in cloud tend to be aggressive about their adoption of cloud. For example, in the survey of 101 IT professionals, the group that was most aggressive about cloud adoption, and which consistently selected 100 percent cloud configurations for the CRM and PCI scenarios were those with less than 25 percent of their time spent on clouds. As experience and usage of cloud increased, the tendency to select 100 percent cloud configurations for both scenarios. These results support hypothesis number two, which states that deep knowledge of cloud security can have a conservative effect on the adoption of cloud services. When we looked at those who took the most conservative approach to cloud adoption, we noticed that years of IT experience had a significant bearing on the attitude towards cloud adoption. The data shows that the more IT experience the participant had, the more likely the individual was to behave cautiously towards cloud adoption. We cannot be sure if this result is due to actual IT experience, or to a generation gap that may not be revealed by the data.

6.4 *Workloads for clouds*

Cloud computing has excellent usefulness, and benefits for many workloads, but not every remedy can advantage from this design, because of some constraints, an example workloads with great stages of security and compliance, specifications can deal with many challenges, requirements can confront many challenges, trying to satisfy strict regulatory mandates, when these workloads are run on clouds. Workloads with low latency requirements, can deal with limitations using the Online, which is the standard accessibility route for cloud, even using a personal network, some programs would not be a good fit for cloud, an example, and some programs have local space for storage

that conventional hardwired straight to avoid shield setbacks. Reaction here we are at these programs is predicted to be near real-time. In addition, workloads with data locality specifications can deal with issues since not all cloud suppliers are able to ensure the location of space for storage and processor chips. Cost is another critical facet to take into account for cloud workloads. An example, programs with large data source should try to get their handling web servers to be collocated with their data storage space in the same cloud. On the other hand, if possible, to avoid additional network charges, they should be collate within the same cloud pod. In addition, in the analysis Of the Cloud Business Risks Framework, we outlined that workloads with unforeseen mountains and cyclical requirements can significantly advantage economically from the cloud model

This financial advantage is draw from the cost reductions of only paying for the service needed, instead of making a large upfront capital investment to support the required but only occasional peak volume one of the workloads that can encounter important price decrease from shifting to a cloud computing service is a “bursty” amount of work. We described earlier the “bursty” design as an amount of work with unforeseen mountains like one caused by flash crowd giving answers to an advertising or special sales offer on an ecommerce webpages. Bursty styles can also be designed through foreseeable demands such as time-of-day, day-of-the-week, or cyclical styles like tax season Bursty workloads benefit from the elasticity versatile settings, and low price storage space of cloud that can manage large potential development in an automated way and at affordable cost. But bursty workloads that manage delicate information and have strict compliance specifications might want to proceed with conventional IT, or make a private cloud The research of 101 IT professionals shows that most believe that workloads like social media programs, exclusive PC, and development and test workloads are the most convenient to move to the cloud computing . Cloud experts questioned for this research believe the fact with that assessment they add the insight that these types of workloads have a lot to benefit from moving to the clouds. For example, social networking applications tend to be bursty workloads, and using cloud technology can help lower the cost of the IT. This is why most, if not all, social

networking solutions like Facebook and LinkedIn, are based on cloud technology. Test and development workloads also benefit from a cloud environment because of their transient nature. When a department is testing a solution, it usually needs many VMs, but after the test is done, the VMs are no longer need. Clouds are good for short-term or fluid projects because they can leverage the transient nature of clouds and minimize upfront costs to most business. The experts also highlighted that desktop clouds are of great value to corporations because this is a way to standardize employees' desktops, enforce patch management, and perform security scans automatically, without needing the cooperation of the end users. Cloud's automation tools, high standardization, and automatic administration of patches are fantastic advantages that virtual desktop applications can exploit when they move to the clouds. In addition, there are business advantages to corporations that use desktop clouds. For example, the risk of employees losing their desktop is eliminated, desktop images can be scanned regularly for malware when the virtual desktops are idle, and adding an employee to the company is as simple as creating a VM instead of having to worry about procuring physical devices. The second number of workloads we will talk about has a method stage of problems to shift to cloud computing. These workloads are not as simple to shift to cloud as the team we just mentioned, but they still usually produce some important advantages from cloud surroundings. The research of IT experts recognized some of these workloads with

6.5 Some warnings when handling cloud images

Some of many new compliance and security problems that can appear if cloud-computing images are not handled and controlled effectively. This area talks about the way new, practical, and (user-friendly) cloud images can be used as equipment to set up harmful application, if no procedure put in position to avoid this new weaknesses.

6.6 Future and early work on cloud computing

Interesting new research is investigating alternatives to address the cross VM side channel and hypervisor escape vulnerabilities, this research is to look at innovative ways to create better security by investigating new options not previously explored. Since most clouds run on x86 processors, finding a Solution that could truly guarantee

isolation within that architecture would be very beneficial. Since this processor, extension contains the infamous interfaces exploited by many malicious rootkits. Rootkits are able to partition a segment of the CPU capacity and lock down memory sectors away from the operating system, using the SMM interfaces. This is the way that rootkits are able to go undetected by average antivirus software.

The University of North Carolina, has existing with IBM Research new technique, and where tries the tables on attackers, by applying the same methods, but this time as a way to secure cloud users (76). This new secure environment enabled by SMM is called “Strong Isolated Computing Environment” (SICE), and it is essentially a sandbox with server resources locked and isolated from the operating system. The new sandbox software consists of only 300 lines of code. Primary amounts show an average overhead of only 3% very well worth the added security system this strategy can provide. The code size is an important point since the more layers, and code created, the more surfaces of attack there are. SICE looks promising as it sections the memory in a fashion that blocks from the operating process, as effectively as your hypervisor. Stopping off this hypervisor contains the added possible of closing the weaknesses discussed earlier on cross-VM side channels and hypervisor escape. If the host is multi-core, SICE sections off one of the cores from the rest of the processor to run the secure sandbox. This is a very promising option to run secure workloads alongside unsecure loads, but it is still early in the development process and much testing remains to be done. We need to keep in mind that the SMM interfaces were design for system management functions, and not for security. However, this research opens the door to new possibilities and designs for future processors with secure layers.

These layers could be carved off through low-level functions to obtain complete isolation with a system that runs other unsecure loads. After extensive review of the survey results, detailed evaluation of best workloads for clouds, and other interesting cautionary stories about the management of cloud images, we are ready to conclude this research with a summary of the findings and conclusions. The next chapter will review the conclusions that rationalize some of our key findings

7. Conclusion

This research has expanded the collective knowledge about cloud computing risks and reducing strategies associated with cloud security, business and compliance risks vectors. By discussions with experts, all cloud risks and reducing methods introduced in the thesis help to rationalize cloud risks and guide IT professionals in what to look for when considering the adoption of cloud computing in the enterprise. Finally, the research goals listed were:

1. The research has created three frameworks:
 - I. The Cloud Security Risks Framework (CSRF).
 - II. The Cloud Business Risks Framework (CBRF).
 - III. The Cloud Compliance Risks Framework (CCRF).
2. In addition, this research illustrated the way financial benefits of the cloud can fluctuate depending on the kind of workloads.
3. The potential financial aids of cloud could be significant, in the meantime substantial reduction in IT cost can be achieved by utilizing the lowest possible configuration and dynamic provisioning of VMs to support demand peaks.
4. Extensive interviews with security and cloud experts provided insights on cloud security, business, and compliance risks. Analysis on the data provided by the experts and consensus-driven Delphi method with the control group helped to rationalize cloud risks and compare these risks with those found in traditional IT.
5. With the intention to guide, IT professionals on their cloud adoption plans, a series of reducing recommendations were provide for each of the risk vectors identified by this research.
6. However, it was not the intention of this research to provide a comprehensive list of reducing alternatives, but instead to offer sufficient reducing options to assist IT professionals with their cloud risks evaluations, and tradeoff decisions between business benefits and security and compliance risks.

The frameworks of this research created based on the large amounts of data, offered by the experts, are expected to be used by IT managers as a way to rationalize many risks.

Association with cloud computing will help to understand cloud computing risk vectors, and to prove that cloud risks are a combination of new risks, as well as prior risks already existing in traditional IT.

In the literature review, many of the current risks prevalent on clouds as well as traditional IT, and under the Cloud Security Risk Framework, the new cloud-specific security risks, such as multitenancy and automation risks were discussed.

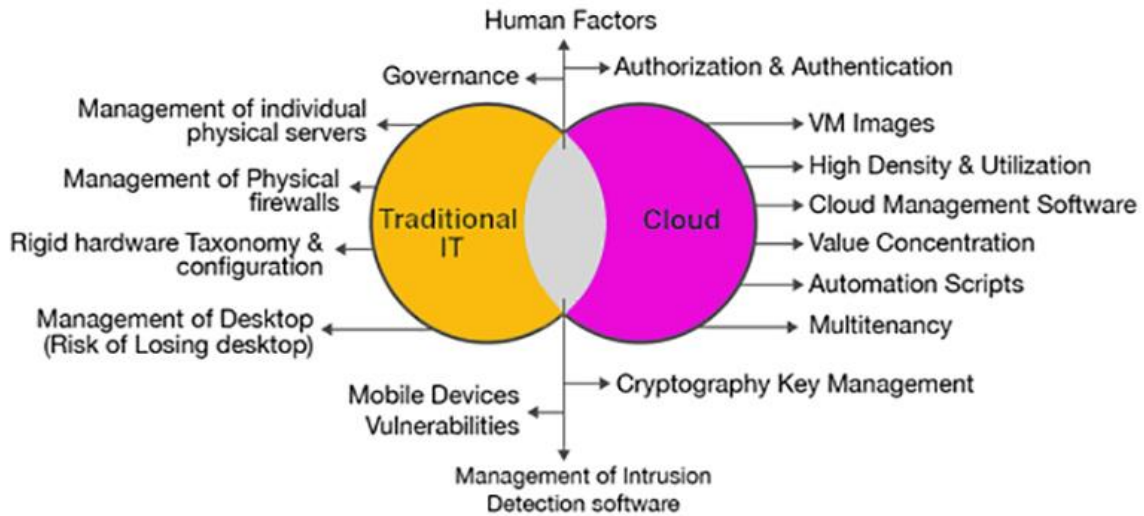
New cloud compliance risks related to cyber forensics, data segmentation, and data remnants are a few of the many new risks associated with clouds, and described under the Cloud Compliance Risks Framework.

Associated with clouds, and described under the CCRF. In addition, we discussed some of the risks that remain exclusively on traditional IT, such as high upfront capital investment for new IT services, and the ever increasing operational cost of proprietary configuration of traditional IT. Based on the substantial data collected by this research, and the analysis of the three frameworks offered by this investigation we can conclude that:

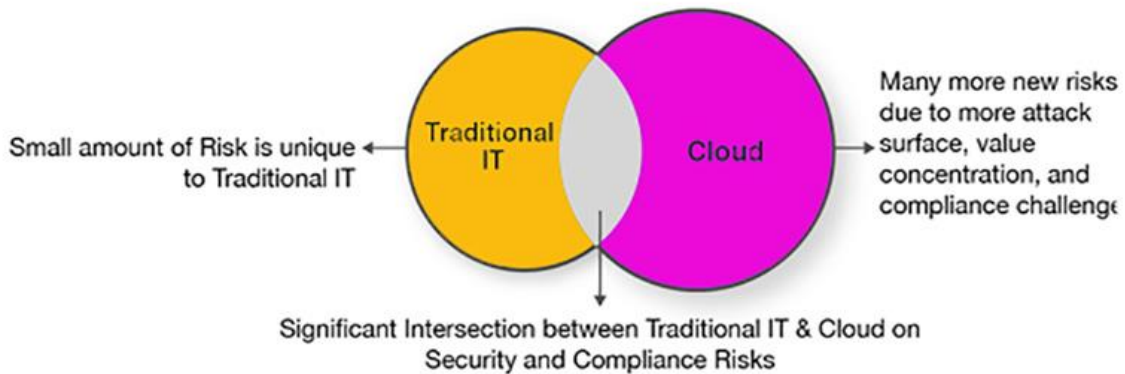
1. Many cloud computing risks are distinctly different from traditional IT risks, that traditional IT still has unique risks that differ from cloud computing,
2. In addition, that there are some of risks that are shared across both environments, creating what we can consider an intersection of risks between cloud and traditional IT.
3. We can conclude that the vectors from the business and compliance cloud models have aggregate total risks higher than traditional IT. From the data

obtained by this research, the Cloud Security Risk Framework, and the Cloud Compliance Framework, We have sufficient evidence to conclude that clouds have substantially higher risks than traditional IT in the areas of security and compliance figure 22.

Figure 22 Cloud Security and Compliance Risks Model



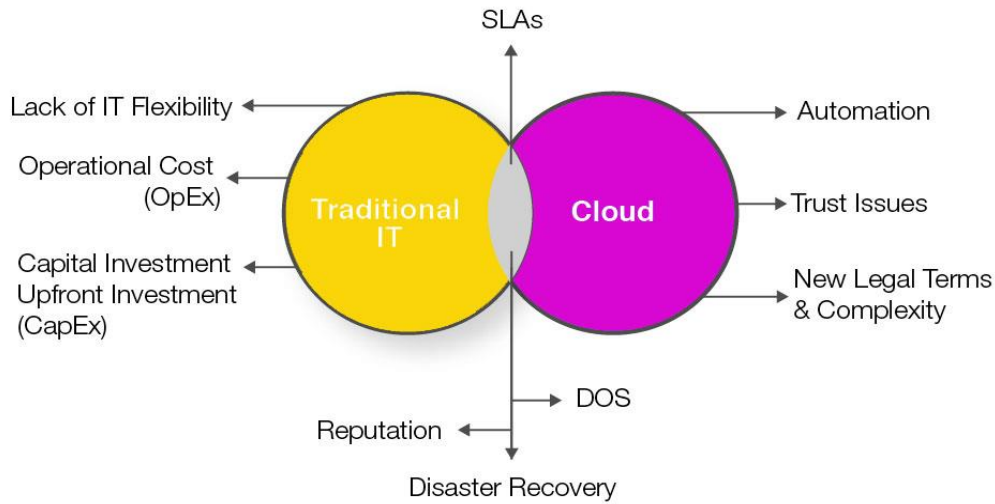
Security and Compliance Model has more Cloud risks with Significant Intersection with Traditional IT



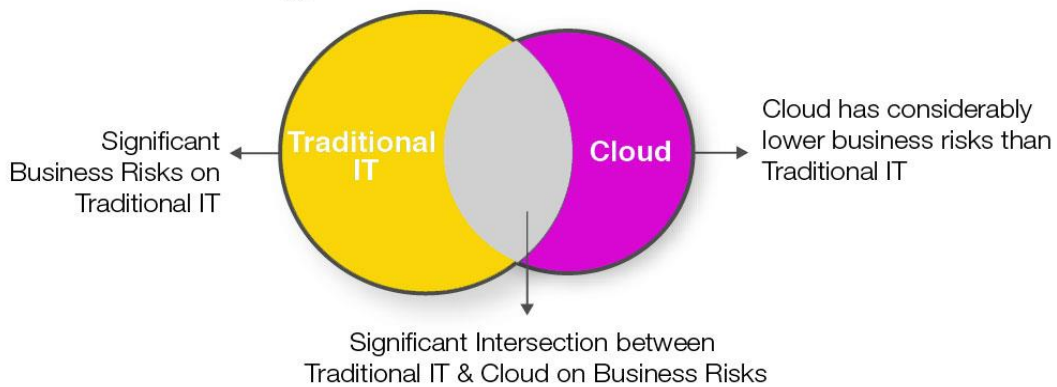
Source Author

Following the same logic on the business side, what is shown to us that the CBRF tends to have vectors with aggregate risks lower than traditional IT, Some of the vectors driving higher business risks on Traditional IT are presented in Figure 23

Figure 23 Cloud Business Risks Model



Business Model has More Traditional IT risks with Significant Intersection with Cloud



Source Author

For each of the threat vectors, the analysis offered some stage of suggestions to reduce the risk. In accordance with the many minimization techniques provided, the fast speed with which cloud computing technological innovation is improving, and the significant economic advantages of the cloud business, we can conservatively predict that many of the cloud risks uncovered by this research will diminish over time, and clouds will become a much safer place to outsource company IT services.

This research found several areas that could benefit from additional research. For example, there is a wealth of additional research that should be done on how to improve cyber forensics tools and methodology in cloud environments.

The dynamic aspects of clouds have created many challenges for cyber forensics practitioners, and there are not too many mitigation strategies to contain this risk vector. In addition, this research did not investigate the claims from some of the experts on possible correlation between best practices and the cost to transform the business to adhere to new regulatory compliance rules, but this could be interesting future research.

Since the pace of technology is very fast in the area of cloud computing, it would be

It would be interesting to do an evaluation of cloud risks in several years to show how risk vectors, identified by this research, have changed with new technologies. We suggest that many current risk vectors are very likely to have lower risk levels in the future, but new vectors will appear and others, like the human factor, will remain the same.

8. References

1. P.Hochmuth. *cloud security survey*. s.l. : IDC, 2011.
2. IDC. *Data center and cloud computing survey*. s.l. : IDC, 2010.
3. Roman T, Lamas,William Stofega. *Worldwide smartphone 2013-2017 forecast and analysis* . s.l. : IDC, 2013.
4. IDC. *data center and cloud computing survey* . s.l. : IDC, 2010.
5. Peter Mell, Timothy Grance. The NIST Definition of Cloud. *National Institute of Standards and Technology*. [Online] September 2011.
<http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>. 800-145.
6. Lydia Leo, Neil MacDonald. *Cloud IaaS: Security Considerations*. G00210095 : Gartner, March,2011. <http://www.chinacloud.cn/upload/2011-11/11113019588314.pdf>.
- 7.M, Azua,. *The Social Factor : Innovate, Ignite, and Win through mass collaboration and social networking*. s.l. : IBM press, 2009.
8. TeleGeography's. *GLOBAL BANDWIDTH RESEARCH SERVICE EXECUTIVE SUMMARY*. s.l. : TeleGeography's, 2013.
http://www.telegeography.com/page_attachments/products/website/research-services/global-bandwidth-research-service/0003/8368/gb13-exec-sum.pdf.
9. M. Weilage. Mary's Shoebox2", *techrepublic*. [Online] April 5, 2010. [Cited: march 5, 2013.] <http://www.techrepublic.com/photos/marys-shoebox2/280735?seq=108&tag=content;siu-container#photopaging>.
10. (GENERIC) (GENERIC) C. Wolf. Apples, Oranges, and Hypervisor Price Comparisons Chris. Apples, Oranges, and Hypervisor Price Comparisons Chris Wolf's Virtualization Tips and Ramblings,. *C. Wolf*. [Online] april 2008. [Cited: December 15, 2012.] <http://www.chriswolf.com>.
11. *Cloud Computing Vs. Grid Computing*. Seyyed Mohsen Hashemi, Amid Khatibi Bardsiri. Tehran, IRAN : ARPJ Journal of Systems and Software , 5,may,2012. 2222-9833 .
12. google. google trends. [Online] 2013.
13. *.worldcommunitygrid*. [Online] [http://www.worldcommunitygrid.org/.](http://www.worldcommunitygrid.org/)
14. N. G. Carr. IT Doesn't Matter. <http://utminers.utep.edu>. [Online] may 1, 2003. [Cited: January 2, 2013.] <http://utminers.utep.edu/kbagchi/itdoesntmatter.pdf>.
15. JeffreyDeanand, SanjayGhemawat. MapReduce: Simplified Data Processing on Large Clusters. [Online] 2008. [Cited: december 25, 2012.] http://static.usenix.org/event/osdi04/tech/full_papers/dean/dean.pdf.

16. google. google trends . [Online] 2013. [Cited: 2 25, 2014.]
17. GNU General Public License, version 2. *GNU General Public License*. [Online] january 1991. [Cited: january 25, 2013.] <http://www.gnu.org/licenses/gpl-2.0.html>.
18. KVM. *linux-kvm*. [Online] [Cited: january 25, 2013.] http://www.linux-kvm.org/page/FAQ#What_do_I_need_to_use_KVM.3F.
19. KVM on illumos. *The Observation Deck*. [Online] August 15, 2011. [Cited: january 25, 2013.] <http://dtrace.org/blogs/bmc/2011/08/15/kvm-on-illumos/>.
20. *Challenges in Building Large-Scale*. Dean, Jeffrey. s.l. : Conference on Web Search and Data Mining (WSDM), 2009.
21. Etkins, Jon. Understanding ephemeral storage. *IBM.com*. [Online] Feb 9, 2011. [Cited: january 29, 2013.] <http://www.ibm.com/developerworks/cloud/library/cl-ephemeralstorage/>.
22. Sanjay Ghemawat, Howard Gobioff, and Shun-Tak Leung. *The Google File System*. s.l. : GooGle, http://static.googleusercontent.com/external_content/untrusted_dlcp/research.google.com/de//archive/gfs-sosp2003.pdf.
23. Vaughan-Nichols, Steven J. What Google's Data Center Can Teach You. *linuxtoday.com*. [Online] [Cited: march 12, 2013.] http://www.linuxtoday.com/high_performance/2010082503135NWSVNT.
24. Dean, Jeff. *Software Engineering Advice from*.
25. CSA, Cloud Security Alliance. *Top Threats to Cloud Computing*. s.l. : CSA, 2010. <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>.
26. suton, Michael. *Top Cloud Threats v2.0*. s.l. : CSA, 2010. <http://365.rsaconference.com/servlet/JiveServlet/previewBody/2819-102-1-3558/STAR-205%20Cloud%20Security%20Alliance%20-%20Top%20Threats%20to%20Cloud%20Computing%20v2.0.pdf>.
27. CSA. *The Notorious Nine Cloud Computing Top Threats in 2013*. s.l. : CSA, February 2013. https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.
28. J. Oberheide, E. Cooke and F. Jahanian,. *Empirical Exploitation of Live Virtual Machine Migration*. s.l. : University of Michigan, . <http://www.blackhat.com/presentations/bh-dc-08/Oberheide/Whitepaper/bh-dc-08-oberheide-WP.pdf>.
29. Leyden, John. Crypto boffins uncover rogue task risk on Amazon cloud. 27,October,2011, http://www.theregister.co.uk/2011/10/27/cloud_security/.

30. Michael McIntosh, Paula Austel. *XML Signature Element Wrapping Attacks and*. s.l. : IBM Research Division, 9, August, 2005.
[http://domino.research.ibm.com/library/cyberdig.nsf/papers/73053F26BFE5D1D385257067004CFD80/\\$File/rc23691.pdf](http://domino.research.ibm.com/library/cyberdig.nsf/papers/73053F26BFE5D1D385257067004CFD80/$File/rc23691.pdf).
31. S. Orrin. *From Virtualization vs. Security to Virtualization Based Security*. s.l. : ISACA, INTEL, 2007.
32. Site, OAuth community. *OAuth community Site*. [Online] [Cited: april 3, 2013.]
<http://oauth.net/>.
33. PCI. *PCI Data Security Standard (PCI DSS)*. 2011. V2,.
34. IBM. "*IBM X-Force 2010 Trend and Risk Report*". s.l. : IBM, March, 2011.
<http://public.dhe.ibm.com/common/ssi/ecm/en/wgl03007usen/WGL03007USEN.PDF>
 .
35. —. *IBM X-Force® 2010 Mid-Year Trend and Risk Report*. s.l. : IBM, August, 2010.
<ftp://public.dhe.ibm.com/common/ssi/ecm/en/wgl03003usen/WGL03003USEN.PDF>.
36. Report, IBM X-Force® 2011 - Mid-year Trend and Risk. *IBM*. s.l. : IBM, September, 2011.
<http://public.dhe.ibm.com/common/ssi/ecm/en/wgl03009usen/WGL03009USEN.PDF>
 .
37. B, Cross. Williams and T. *Virtualization System Security*. s.l. : IBM, 2010.
<http://blogs.iss.net/archive/papers/VirtualizationSecurity.pdf>.
38. Younan, Yves. *25 Years of Vulnerabilities 1988-2012*. s.l. : Sourcefire Vulnerability Research Team (VRT), 2013. 2.13 | REV1.
39. S, Song. K. Crook and I. *Mobile Virtualization Technology Assessment*. s.l. : IDC, 2011.
40. KVM- KERNEL BASED VIRTUAL MACHINE. *www.redhat.com*. [Online] 2009. [Cited: April 19, 2013.] <http://www.redhat.com/rhcm/rest-rhcm/jcr/repository/collaboration/jcr:system/jcr:versionStorage/5e7884ed7f00000102c317385572f1b1/1/jcr:frozenNode/rh:pdfFile.pdf>.
41. Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage. Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. *http://www.cs.cornell.edu*. [Online] November 9-13, 2009. [Cited: April 19, 2013.] <http://www.cs.cornell.edu/courses/cs6460/2011sp/papers/cloudsec-ccs09.pdf>. ACM 978-1-60558-352-5/09/11.
42. IDC. Strong Demand for Smartphones and Heated Vendor Competition Characterize the Worldwide Mobile Phone Market at the End of 2012, IDC Says . *http://www.idc.com*. [Online] IDC, January 24, 2013. [Cited: april 25, 2013.] <http://www.idc.com/getdoc.jsp?containerId=prUS23916413#.US6A9zd4Dla>.

43. Ghemawat, Jeffery Dean and sanjeey. MapReduce: simplified data processing on large. *Google.ing*. 2008, Vol. 51,
http://static.googleusercontent.com/external_content/untrusted_dlcp/research.google.com/ar//archive/mapreduce-osdi04.pdf.
44. REPORT, GLOBAL FRAUD. *2012-2013 KROLL GLOBAL FRAUD REPORT SURVEY EXECUTIVE SUMMARY*. s.l. : GLOBAL FRAUD REPORT, 2013.
http://www.krolladvisory.com/library/2012-2013_Global_Fraud_Report_Executive_Summary_FINAL.pdf.
45. Post Mortem: What Happened During the Amazon Outage .
<http://blog.saplinglearning.com>. [Online] April 29, 2011. [Cited: may 12, 2013.]
<http://blog.saplinglearning.com/2011/04/post-mortem-what-happened-during-amazon.html>.
46. *Enabling smarter compliance architecture using social networks and cognitive agents*. Goodman, M. Azua and B. 0018-8646 , s.l. : IBM Journal of Research and Development, 2011.
<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6099648>.
47. Gabriela Gheorghe, Fabio Massacci,Alexander Pretschner. GoCoMM: A Governance and Compliance Maturity Model. *www.artdecode.de*. [Online] [Cited: December 25, 2012.] <http://www.artdecode.de/Papers/GoCoMM.pdf>.
48. Matthew Scholl, Kevin Stine,Joan Hash, Pauline Bowen, Arnold Johnson,Carla Dancy Smith, and Daniel I. Steinberg. *An Introductory Resource Guide for Implementing the HIPPS Security Rule*. <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf> : National Institute of Standards and Technology, 800-66 Revision 1, 2008.
49. *The Modified Delphi Technique - A Rotational Modification*. Rodney L. Custer, Joseph A. Scarcella,Bob R. Stewart. Spring 1999, Vols. Volume 15, Number 2.
50. *The Delphi Method for Graduate Research*. Gregory J. Skulmoski, Francis T. Hartman and Jennifer Krahn. s.l. : Journal of Information Technology Education , 2007, Vols. 6, 2007. <http://informingscience.org/jite/documents/Vol6/JITEv6p001-021Skulmoski212.pdf>.
51. Mcheal . Adler and Erio. Ziglio. *Gazing Into the Oracle: The Delphi Method and Its Application to Social ...* s.l. : Jessica Kingsley Publishers,, 1996. 185302-1040.
52. Chitu Okoli and Suzzane D. Pawlowski. The Delphi method as a research tool: an example, design considerations and applications. *www.sciencedirect.com*. [Online] 2004. [Cited: December 5, 2012.]
<http://www.sciencedirect.com/science/article/pii/S0378720603001794>.
53. Dalkey, Norman C. The Delphi Method: An Experimental Study of Group Opinion. <http://www.rand.org>. [Online] 1969. [Cited: December 5, 2012.]

http://www.rand.org/content/dam/rand/pubs/research_memoranda/RM5888/RM5888.pdf. RM-588-PR.

54. Gene Rowe, George Wright. The Delphi technique as a forecasting tool: issues and analysis”, International Journal of Forecasting. *www.forecastingprinciples.com*. [Online] 1999. [Cited: December 6, 2012.] <http://www.forecastingprinciples.com/files/delphi%20technique%20Rowe%20Wright.pdf>. 353-375.

55. *Mental Models of Privacy and Security*. Camp, L Jean. s.l. : IEEE Technology & Society, , 2006. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=922735.

56. *An Investigation of Decision-Making and the Tradeoffs*. Farkas, L. Chen and D. s.l. : 15th Americas Conference on Information, 2009.

57. *The Social Factor: Innovate, Ignite, and Win through mass Collaboration and Social Networking*. Azua, Maria. 978-0-13-701890-1, Upper Saddle River, : IBM Press, Vol. 13.

58. *Cloud computing*. Dean Frantsvog, Tom Seymour, Freneymon John,. s.l. : International Journal of Management & Information Systems, 2012, Vol. 16.

59. Morton, Dave. IBM Mainframe Operating Systems: Timeline and Brief Explanation. December 2014, Vol. Version 37.2.

60. An open protocol to allow secure authorization in a simple and standard method from web, mobile and desktop applications. *OAuth*. [Online] [Cited: 08 12, 2014.] <http://oauth.net/>.

61. CHAPPELL, DAVID. *Introducing the Azure Services Platform*. october 2008.

62. Himanshu Dwivedi, Zane Lackey, Jesse Burns. *Hacking Exposed Web 2.0: Web 2.0 Security Secrets and Solutions*. December 17, 2007. ISBN-10: 0071494618.

63. *Failure Trends in a Large Disk Drive Population*. Eduardo Pinheiro, Wolf-Dietrich Weber a, Luiz Andr. Mountain View, CA 94043 : s.n., February 2007.

64. Editor, Joan Goodchild and Senior. Most fraud is an inside job, says survey. <http://www.csoonline.com>. [Online] 2011. [Cited: 10 5, 2014.] <http://www.csoonline.com/article/2130085/fraud-prevention/most-fraud-is-an-inside-job--says-survey.html>.

65. Kevin D. Mitnick, William L. Simon, Steve Wozniak. *The Art of Deception: Controlling the Human*. October 2002. ISBN: 978-0-471-23712-9.

66. Service Provider Administrator Guide. *safenet*. [Online] 7 18, 2013. [Cited: 1 15, 2015.] <http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-ServiceProviderAdministratorGuide.pdf>. Version 3.3.

67. Brodtkin, Jon. Burning question: How can security risks be mitigated in virtualized systems? *international news*. [Online] 10 25, 2010. [Cited: 11 29, 2014.] <http://news.idg.no/cw/art.cfm?id=E3B6DE73-1A64-67EA-E4CD42C65CF77E6D>.
68. Vogels, Werner. Expanding the Cloud - Introducing Amazon ElastiCache. [Online] 09 22, 2011. [Cited: 11 30, 2014.] <http://www.allthingsdistributed.com/2011/08/amazon-elasticache.html>.
69. Parker, Bob. *IDC Manufacturing Insights: IT Strategies*. Framingham : IDC Manufacturing Insights, June 2011. MI228939.
70. Cruz, Xath. Cloud Case Studies: The Animation Industry. *Cloud times*. [Online] january 19, 2013. [Cited: january 1, 2015.] <http://cloudtimes.org/2013/01/19/cloud-case-studies-the-animation-industry/>.
71. Preimesberger, Chris. nine Reasons for Cloud Application Failure. *www.eweek.com*. [Online] 08 13, 2014. [Cited: 1 5, 2015.] <http://www.eweek.com/cloud/slideshows/nine-common-reasons-cloud-systems-crash.html>.
72. Tim Mather, sushahed Latifbra Kumaraswamy ,. *Cloud security and Privacy* . s.l. : "O'Reilly Media, Inc, 04/09/2009. 978-0-596-802769.
73. *CRITICAL FACTORS AFFECTING THE UTILIZATION OF CLOUD COMPUTING*. Alberto Daniel Salinas Montemayor, Jesús Fabián López, Jesús Cruz Álvarez. 2014, Vol. 2. 1805-9961.
74. *Conflict translates environmental and social risk into business costs*. Daniel M. Franks. Rachel Davis, Anthony . J ,saleem H Ali , Deanna Kemp ,Martin Scurrah. March 19, 2014, Vol. 111 no. 21. 1405135111.
75. Cloud Server Comparison. *clouorado*. [Online] [Cited: 28 1, 2015.] <https://www.clouorado.com> price comparison engine like Clouorado.
76. *Base: An Acid Alternative " In partitioned databases, trading some consistency for availability"*. Pritchett, Dan. 2008. 1542-7730/08/0500.
77. Brian Honan, Jim Reavis, Raj Samani. *CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security* . s.l. : Cloud Security Alliance csa, 2014-10-08 . 9780124201255 .
78. *Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds*. Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage. Chicago ,usa : ACM Conference on Computer and Communications Security, 9-13 /11/ 2009. 978-1-60558-894-0.
79. Leyden, John. Crypto boffins uncover rogue task risk on Amazon cloud AWS drops the SOAP, plugs backdoor quickly though. *www.theregister.co.uk*. [Online] october 27, 2011. [Cited: jan 13, 2013.] http://www.theregister.co.uk/2011/10/27/cloud_security/.

80. Michael McIntosh, Paula Austel. XML signature element wrapping attacks and countermeasure. *http://journalogy.net*. [Online] 2005. [Cited: january 19, 2013.]

9. Appendix A

cloud computing risks and frameworksQz					
Survey					
1.How would you rate your level of expertise on the following ?					
	Expert	Knowledgeable user	Novice user	Educated	Unfamiliar
Cloud computing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
IT security	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2. How many years of IT professional experience do you have?

- More than 25 years
- 16 to 25years
- 5to 15 years
- 5 to 10years
- less than 5 years
- No experience at all

3. How many years of professional experience do you have using or designing cloud computing services?

- More than 4 years
- 3 to 4 years
- 1 to 2 years
- Less than 1 year
- No experience at all

4.What the deployment models of cloud you using ?

- Privet cloud
- Public cloud
- Hybrid cloud
- Community cloud

5. From the perspective of an IT provider, rate the level of IT risks associated with these cloud technologies and trends compared to Traditional IT?

	Substantially increases risk	Moderately increases risk	No change in risk	Moderately decreases risk	Substantially decreases risk	No idea
Visualization technologies (e.g. Hypervisors, visualized networks)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Distributed Storage (e.g. Storage clouds, Files stored multiple times for world wide availability)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Distributed Databases (e.g. Eventually consistent databases, not SQL/Relational databases)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Authentication and Authorization (e.g. ACLs for Billions of records)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mega IT Data Centers (e.g. Consolidation of many data centers into gigantic cloud Data Centers)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Self-service IT Model (e.g. New single point of VM management)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mobile Applications (e.g. Location--Based Range Queries)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Automation (e.g. scripts and interfaces for VM workflow automation)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cloud open standards (e.g. OVF, OCCI)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Human Factors (e.g. human error, and insider threats)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

6. From the perspective of a Cloud consumer, rate the importance of these cloud computing services for your business?

	Top important	Important	Moderately important	Little important	No Idea
Reduce IT capital investment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reduce cost of IT operations	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Improve availability of application	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provide flexibility to scale up during peak demand cycles	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Support of mobile devices	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Leverage cloud platform APIs to reduce development cost	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provide flexible payment schedule	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Maintain high quality service to preserve reputation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Preserve security standards	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Maintain Security Compliance certification	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

7. Rate the level of effort required to move these workloads to a cloud infrastructure ?

	Very difficult	Difficulty	Medium difficult	Easy	Very easy	No Idea
Social Networking Applications	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
eCommerce Applications	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data Analytic	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Virtual Desktop	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Development and Test workloads	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data Intensive Applications with residency/sovereignty compliance requirements	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Healthcare applications with HIPAA compliance requirements	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Legacy application	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Banking Transactions Reconciliation Services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Customer Relationship Management (CRM)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

8. Select the statement that best describes your thinking about cloud vulnerabilities ?

- Cloud can strongly support mission critical applications and doesn't create any new vulnerabilities.
- Cloud can support some mission critical applications but it creates some new vulnerabilities.
- Cloud is not ready for mission critical applications due to many new security vulnerabilities.
- No Idea

9. Select the statement that best describes your thinking about cloud automation ?

- Cloud automation increases the effectiveness of system administrators.
- Cloud automation doesn't affect the effectiveness of system administrators.
- Cloud automation lowers the effectiveness of system administrators because it is complex technology.
- No idea

10. Assume you are an IT manager responsible for deploying a new Customer Relationship Management (CRM) solution. What option would you select?

- Use Traditional IT - Acquire capital to cover maximum peak capacity expected.
- Use Hybrid Cloud - Acquire capital for average capacity. Use cloud services for peak demand.
- Use 100% Cloud - Relinquish physical server control and leverage a cloud with CRM services.
- No idea

11. Assume you are an IT manager responsible for compliance with the Payment Card Industry (PCI) data security standard. What option would you select ?

- Use Traditional IT - Acquire capital and software for credit card payment service.
- Use Hybrid Cloud – Connect business solution to cloud credit card payment service.
- Use 100% Cloud - Move business solution to a cloud with integrated PCI service.
- No idea

12. How important is cloud computing to your company ?

- Very important – Is one of the top priorities and currently fully enabling our business to use cloud computing
- Important – Is a significant goal and currently enabling part of the business to use cloud computing
- Medium Priority - Is of average importance and some limited usage has taken place.
- Low Priority – Is of little importance but there are plans to adopt this technology in the future.
- Not a Priority – No plans to adopt cloud computing

13. How important is innovation to your company?

- Very important – Is one of the top priorities and part of the culture to create better products and services.
- Important – Is used as an important instrument to improve the business
- Medium Priority - Is of average importance and used to enable competing against rivals.
- Low Priority – Is of little importance and sometimes driven by short-term opportunistic situations.
- Not a Priority – Is NOT important to the business.

14. How important is business governance, in support of regulatory compliance, to your company?

- Very important – Is one of the top priorities and part of the culture to achieve high regulatory compliance.
- Important – Is a significant instrument to achieve regulatory compliance
- Medium Priority - Is of average importance and helps maintain normal industry regulatory compliance.
- Low Priority – Is of little importance and followed to maintain minimum industry regulatory compliance.
- Not a Priority – Is NOT important. The business operates on the edge and regulatory compliance.

15. What percentage of your IT/computing usage is cloud-based or uses cloud services like IaaS/PaaS (e.g. Amazon (AWS), Google apps, IBM SmartCloud, etc. ?


- More than 80%.
- 51% to 80%
- 25% to 50%
- Less than 25%
- I'm not using cloud services

16. What statement best represents your opinion on Social Networking sites (e.g. Facebook, LinkedIn, and Google+)?

- I don't know of any security issues associated with Social Networking sites. I believe these services provide a secure environment to connect with friends
- I'm aware of some small security issues with Social Networking sites but I believe they do a reasonable job at protecting the privacy of their users.
- I'm aware of extensive security issues with Social Networking sites but I'm willing to give up substantial personal privacy in return for social connectivity
- I don't use social networking tools because of extensive security issues.
- I don't use social networking tools.

Submit

100%: You made it.

Powered by
 Google Forms

This content is neither created nor endorsed by Google.

[Report Abuse](#) - [Terms of Service](#) - [Additional Terms](#)

10. Appendix B

List of Experts

COMPANY	POSITION
IBM	Security Expert on malware, analyst and consultant for IBM Internet Security Systems
IBM	Manager of Cloud Technology Innovations
ORACLE CLOUD	Leads Cloud Technology
HP	Cloud Security Lead Architect

11. Appendix C

Results of Framework Calibration

Results from the input provided by experts via the calibration instrument explained in section 3.3 these results provided the basis for the arrows illustrated in the security, business, and compliance frameworks. As shown in the following figures, these experts agreed strongly on how each of the vectors affected cloud computing risks compared to traditional IT.

Figure 24 Results on business risks framework calibration

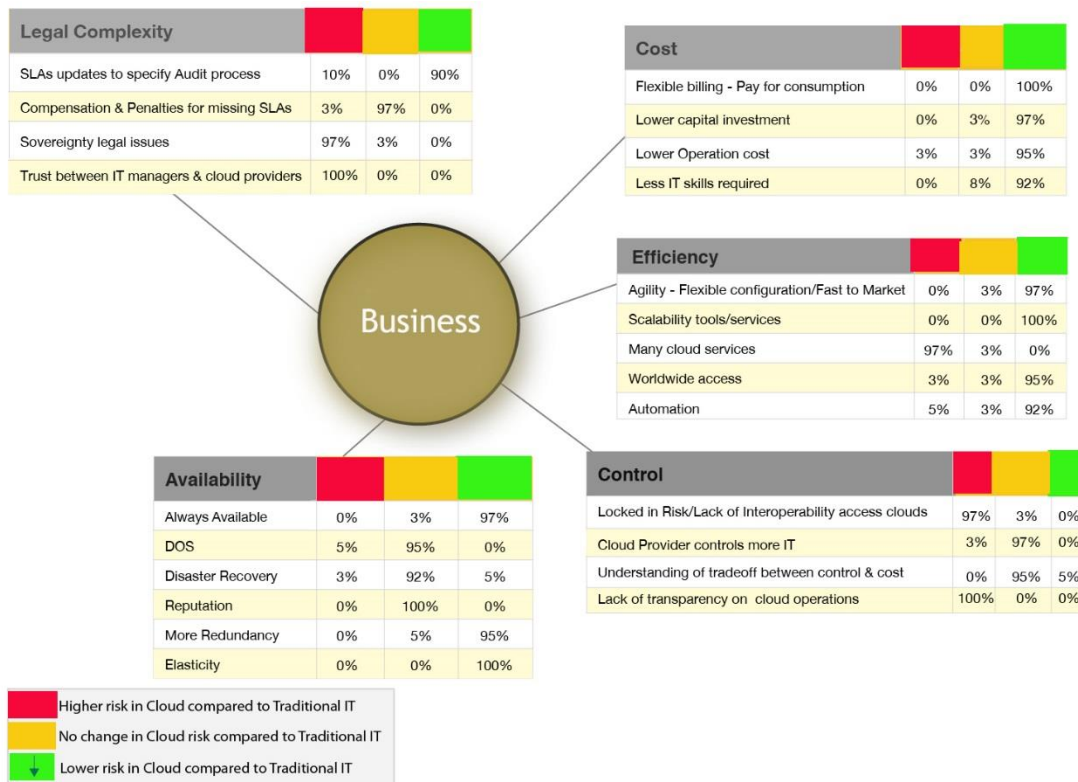


Figure 25 Results on security risks framework calibration

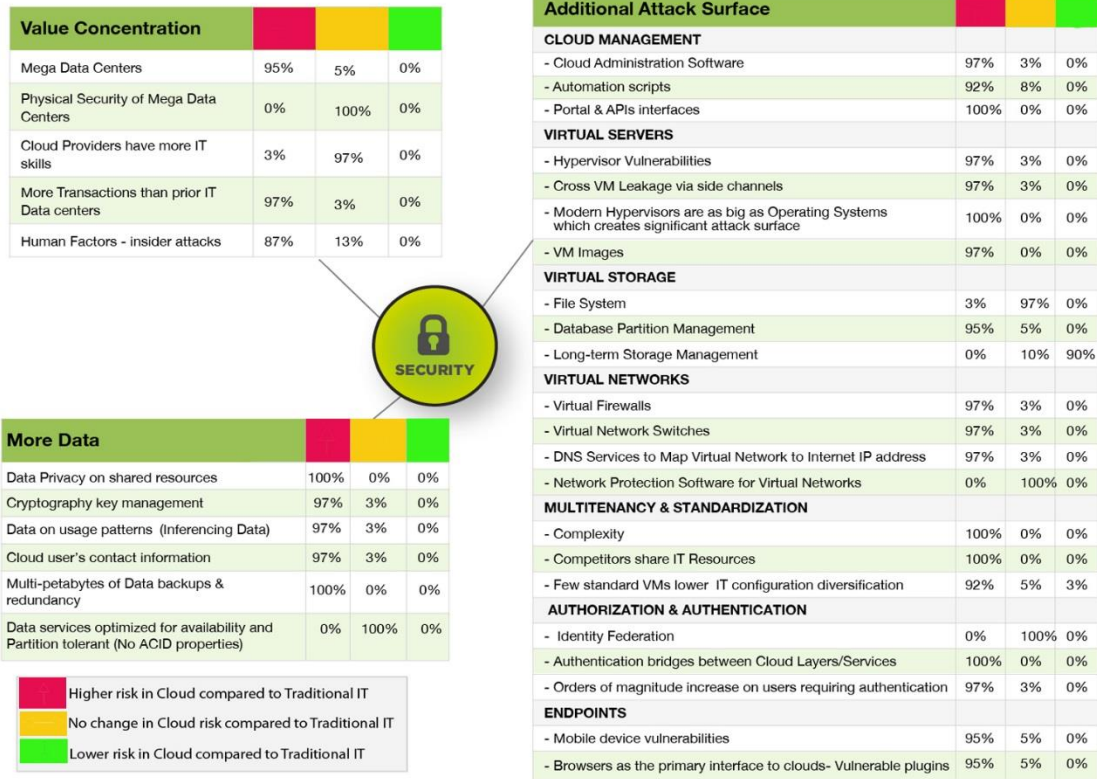


Figure 26 Results on compliance risks framework calibration

