DAVID ESHIEMOKHA ILANI

DESIGN AND IMPLEMENTATION OF RISK ASSESSMENT AND DISASTER RECOVERY PLANS SCENARIO: INFORMATION SYSTEM TECHNOLOGY DATA CENTER IN CLOUD MIGRATION

NEU 2017

DESIGN AND IMPLEMENTATION OF RISK ASSESSMENT AND DISASTER RECOVERY PLAN SCENARIO: INFORMATION SYSTEM TECHNOLOGY DATA CENTER IN CLOUD MIGRATION

A THESIS SUBMITTED TO THE GRADUATE SCHOOL OF APPLIED SCIENCES OF NEAR EAST UNIVERSITY

By

DAVID ESHIEMOKHA ILANI

In Partial Fulfillment of the Requirements for the Degree of Master of Applied Science in Information Systems Engineering

NICOSIA 2017

DESIGN AND IMPLEMENTATION OF RISK ASSESSMENT AND DISASTER RECOVERY PLANS SCENARIO: INFORMATION SYSTEM TECHNOLOGY DATA CENTER IN CLOUD MIGRATION

A THESIS SUBMITTED TO THE GRADUATE SCHOOL OF APPLIED SCIENCES OF NEAR EAST UNIVERSITY

By
DAVID ESHIEMOKHA ILANI

In Partial Fulfilment of the Requirements for the Degree of Master of Applied Science in Information Systems Engineering

NICOSIA 2017

David Eshiemokha ILANI: DESIGNAND IMPLEMENTATION OF RISK ASSESSMENT AND DISASTER RECOVERY PLANS SCENARIO: INFORMATION SYSTEM TECHNOLOGY DATA CENTER IN CLOUD MIGRATION

Approval of Director of Graduate School of Applied Sciences

Prof.Dr. Nadire ÇAVUŞ

We certify this thesis is satisfactory for the award of the degree of Masters of Applied Science in Information Systems Engineering

Examining Committee in Charge:

Assist. Prof. Dr. Huseyin Lort	Department of Computer and Instructional Technology Teaching, GAU (Jury Chairman)
Assist. Prof. Dr. Boran Şekeroğlu	Department of Information Systems Engineering, NEU (Jury Member)
Assist. Prof. Dr. Yöney Kırsal Ever	Thesis Supervisor, Department of Software Engineering, NEU

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name: David Eshiemokha Ilani
Signature:
Date:

To Almighty God and to my Parents …

ACKNOWLEDGEMENTS

This thesis would not have been achievable without the help, support and patience of my principal supervisor Assist. Prof. Dr. Yoney Ever she is a mother and a counsellor. She has walked me through all the stages of the writing of my thesis. Without her consistent and illuminating instruction, this thesis could not have reached its present form, May God bless her. My deepest gratitude goes to Assist. Prof. Dr. Boran Sekeroglu, for his constant encouragement and guidance since the first day I met him; he has been a good mentor.

I would like to thank Prof. Dogan Ibrahim who has been very helpful through the duration of my Thesis and the head of Applied Science Institues, Prof. Dr. Nadire Çavuş for her guideline which help to ease my work and instruction, May God Bless her.

Above all, my infinite thanks and genuine love would be dedicated to my dearest families for their loyalty and their great confidence in me. I am greatly indebted to my Mom Lady Beatrice Athekame, who is indeed my inspiration and the woman who led me to the treasures of knowledge and believed that one day I will be a great man. I would like to thank my best friend and a partner Chinenye Ogbuakanne for giving me a support, patience at all times; encouragement and constant love have sustained me. I would to thank Mr. & Mrs. Elias Igbinakenzua for their love, and encouragement. Also special thanks to Sir. Stan Athekame, for his mentorship. Finally, there is a long list of friends that I would like to thank. I can't mention them all but I would like to thank them from all, my heart for their valuable help and support.

ABSTRACT

In today's World, we have been exposed to numerous disasters and large-scale emergencies; we must always assess our environs, offices and homes in other to avoid anything that may cause arms or disruption of our businesses. With the help of Information systems technology we can prevent and mitigate the effects that may threaten us if applied accurately, Organization must prepared and budget for any form of disasters that may threaten our businesses. Risk assessment is an organized and orderly system, which wards upon the correct identification of risks. Likewise, it is correct assessment of risks emerging from them, with a view to making between hazard correlations for reasons for their control and shirking. There are distinctive in the methodologies used to conduct hazards and evaluations. The Enterprise is a complex of meanings between Services, Business Processes and Applications with Interdependencies.

The contributions of this thesis is a Disaster Recovery Framework that spotlights on relating Application (App) and Infrastructure mappings in the Configuration Management Database, and aligns this information per the Enterprise Architecture Meta-model to discover Interdependencies and App Recovery Time Actual. This can be accomplished utilizing the Recovery Sequence Algorithm that locally organizes the request of recuperation At Time of Disaster with the end goal that it limits cost of downtime to the Enterprise.

This study also focus on the combination of risk assessment and disaster recovery on a single app and how best data center can be managed efficiently, based on both applications can work cyclonically. At last, we talk about the dependability challenges confronted by data centers and present another replication strategy that permits distributed computing stages to offer elite, no-information lost disaster recovery administrations in spite of high system latencies.

Today's data center must scale, be reactive and proactively slice expenses to make due in the new period to enormous information, versatile, online networking and cloud by utilizing distributed computing and virtualization innovation.

Keywords: Risk assessment; information technology; risk management; disaster relief; data center; and cloud computing

ÖZ

Bugünün dünyasında, çok sayıda afete ve büyük ölçekli acillere maruz kaldık; İşlerimizin silahlanmasına veya bozulmasına neden olabilecek herhangi bir şeyden kaçınmak için çevremizi, ofislerimizi ve evlerimizi her zaman değerlendirmeliyiz. Bilgi sistemleri teknolojisinin yardımı ile, doğru uygulandığında bizi tehdit edebilecek etkileri önleyebilir ve hafifletebiliriz. Kuruluşumuz, işletmelerimizi tehdit edebilecek her türlü felaket için hazırlıklı olmak ve bütçelemek zorundadır. Risk değerlendirmesi, risklerin doğru tanımlanmasını gözlemleyen organize ve düzenli bir sistemdir. Aynı şekilde, tehlike korelasyonları arasındaki kontrol ve kaçınma sebeplerinden kaynaklanan risklerin doğru olarak değerlendirilmesi gereklidir. tehlikeleri ve değerlendirmeleri yapmak için kullanılan metodolojilerde belirgin özellikler vardır. Kurum, Hizmetler, iş süreçleri ve bağımlı olmayan uygulamalar arasındaki karmaşık bir anlam ifade eder.

Bu tezin katkısı, yapılandırma yönetim veritabanında uygulama ve altyapı eşlemeleri ile ilgili olarak ortaya çıkan ve karşılıklı bağımlılıkları ve gerçek uygulama kurtarma zamanını keşfetmek için kurumsal mimari meta modeline göre sıralayan bir felaket kurtarma çerçevesidir. bu, Felaket zamanında iyileşme talebini yerel olarak organize eden kurtarma dizisi algoritması'nı kullanarak başarılabilir; bu da, işletme için kesinti maliyetini sınırlandırır.

Bu çalışma aynı zamanda, tek bir uygulamada risk değerlendirmesi ve felaket kurtarma kombinasyonuna ve en iyi veri merkezinin verimli bir şekilde yönetilebilmesine odaklanır; her iki uygulamanın da temelinde, hızlı bir şekilde çalışması mümkündür. Sonunda, veri merkezlerinin karşı karşıya kaldığı bağımlılık zorluklarından bahsediyoruz ve dağıtılmış bilgi işlem aşamalarının yüksek sistem gecikmesine rağmen elit, enformasyonsuz felaket kurtarma yönetimlerini sunmasına izin veren başka bir çoğaltma stratejisi sunuyoruz.

Günümüzün veri merkezi, yeni dönemde dağıtılmış bilgi işlem ve sanallaştırma yeniliklerinden yararlanarak muazzam bilgi, çok yönlü, çevrimiçi ağ ve bulut oluşturmak için masrafları kesmek, reaktif olmak ve proaktif olarak kesmek zorundadır.

Günümüzün veri merkezi, yeni çağda büyük veri, mobil, sosyal medya ve bulut bilgi işlem ve sanallaştırma teknolojisini kullanarak hayatta kalabilmek için ölçeklendirmeli, duyarlı olmalı ve proaktif olarak maliyetleri düşürmelidir.

Anahtar Kelimeler: Risk değerlendirmesi; bilgi teknolojisi; risk yönetimi; afet yardımı; veri merkezi; ve bulut bilgi işlem

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLE

CHAPTER ONE
INTRODUCTION

In life everything is a risk if is not properly managed and if we do not plan well, we fail and sometimes the consequences of improper planning could be unrepairable. In the recent events, many disturbing disasters have been seen all around the world and most of them are still creating huge problem especially in the Europe, North America and Asia part of the world. Shaluf 2007 copes that disasters can be broken down into three main part which are, man-made, natural disaster and hybrid varieties. Josh 2016 point that disaster event is made by characteristic powers, for example, Earthquakes, tidal wave, typhoons and flooding. Man-settled on sorts result from human choices, for example, building breakdown, transport mishaps and war, weapon outfitted men, and some more. The hybrid disaster is the mix of both regular and man-made disaster. A few people trust that the frequency of disasters is on the expansion day by day (Ofori, 2004; Spens, 2007, and Whybark, 2007). Thusly, moreover inquire about has shown estimable. The objective of this research work is to a risk assessment and disasters recovery plans scenario in the field of information systems technology in data center for cloud migration, that contain disaster relief, disaster recovery, data center migration to the cloud and the risk involved in the migration of data and applications into cloud, which help to direct human persisting and return districts to conventionality. This is for the most part a multifaceted undertaking requiring a lot of organization limit and resources openness. Ofori 2004 disputes were that disaster situation extraordinarily influences the developed condition and this is transcendently exacerbated by virtue of best in class countries. This makes a situation where fiscal and disaster recovery in those areas carries various years with the result being deferred continuing of inhabitants. Some of the most recent examples include the Kaikoura (New Zealand) earthquake on 14 November 2016, the Nepal earthquake in 2015 and the Indian Ocean tsunami in 2004.

The utilization of project management has fathomed its community of learning associated with various fields including, boundary, advancement prosperity and data innovation, which is our bone of controversy. Productions for instance, the Project Management Body of Knowledge (PMBoK®) (PMI, 2008), grasps thoughts inside project lifecycles, techniques, frames and the distinctive learning districts. Bolt, (1994) analyzed various systems that exist to administer projects; however the foremost goals continue as before in a respectable way to deal with and

consider project management is similarly as "finishing project objectives with resources accessible".

Risk Assessment is a basic apparatus for any information technology organization managers, to use in the assessing the security of the IT frameworks that they oversee, and in knowing the potential for damage and misfortune to authoritative operations, its main goal and partners. The risk assessment and disaster recovery furnishes administration with the capacity to:

- Meet Federal necessities for dataand framework security.
- Establish a worthy level of hazard.
- Emergency response procedures
- Backup operations procedures
- To provide adequate level of security protection for IT data center, and systems applications
- Recovery actions procedures

In the process of disaster recovery, the main function of risk assessment is to pre-determineas many types of disasters as possible that an organization may come across, and then to figure out how the organization will deal with each crisis if it arises (Ahmad, *2017).*

Disaster, flighty by nature, can strike any place whenever with next to zero cautioning. Recouping from one can be distressing, costly and tedious, especially for the individuals who have not set aside the opportunity to think ahead and get ready for such potential outcomes (Sandra, 2015) bring up that when disaster strikes, the individuals who have arranged and made recuperation arrangements live to tell the story with relatively negligible misfortune or disturbance of creation.

Disasters can take a couple of particular structures. Some basically impact individuals e.g., hard drive emergencies while others have a greater, total impact (Anugra, 2012). Disaster can happen, for example, control blackouts, surges, fires, storms, gear disappointment, damage, psychological oppression, or even pestilence disease. Each of these can be in any event cause hereand now disturbances in typical business operation. Nonetheless, recouping from the effect of large portions of the previously mentioned disaster can take any longer, particularly if associations have not set up ahead of time (Disaster recovery Organization, 2012).

An extensive segment of us see that these potential issues as possible results. Tragically the intervention of some of these disasters quiets a couple of organisations into a sentiment false

security-"that is not inclined to happen here." However, in the occasion that true blue courses of action have been made, the disaster recovery plans arrange does not should be exceedingly irritating. Or maybe, the strategy can be modernized, yet this help of recuperation will simply happen where plans have been made. Organizations that put aside the chance to execute disaster recovery plans of time routinely ride out fiascoes with unimportant or no loss of data, gear, or business pay. In this way its empowers them to keep up the certainty and conviction of their customers and monetary pros (Pillai, 2016).

Disaster Recovery Planning is the variable that has the fundamental impact between the organization that can successfully regulate crises with negligible cost and effort and most outrageous speed, and those that are left snatching the pieces for untold time ranges and at whatever cost providers charge; organizations constrained to settle on decision out of frenzy. Disaster Recovery can be a productive, reliable and less troublesome process if we intertwine two key resources: circulated capacity and Comm vault. (Gralewski, 2017)

Cloud is an adaptable, (typically) reasonable alternative for testing disaster recovery plans. With pay-as-you-go valuing, it is more moderate to turn up cloud assets for a DR test then kill the additional cloud assets when the DR testing is finished. Commvault has full cloud disaster recovery on information management bolster mechanized and available for IT experts (Gralewski, 2017)

Disaster Recovery Plan steps incorporate a general examination of an organization's business frames, IT establishment, data fortification, resources, congruity necessities and disaster recovery activity strategies. It is the route toward making complete reports, which will support organization in recovering from disaster events. Developing a disaster recovery plans shifts between endeavors in light of business sort, frames, the security levels required, and the organization measure. There are diverse stages required in working up a fruitful Disaster Recovery or Business Continuity orchestrating (Bill, 2012). The key stages and the course of action steps are outlined out underneath:

Stage I – Data Collection (2014 Milap Oza)

- Project should be made with course out of occasions, resources, and expected yield
- Business influence examination should be driven at standard intervals
- Risk examination should be driven routinely

- Onsite and Offsite Backup and Recovery methods should be investigated
- Alternate site region must be picked and arranged for use

Stage II – Plan Development and Testing

- Development of Disaster Recovery Plan
- Testing the game plan

Stage III – Monitoring and Maintenance

- Maintenance of the Plan through updates and review
- Periodic examination of DRP
- Documentation of changes

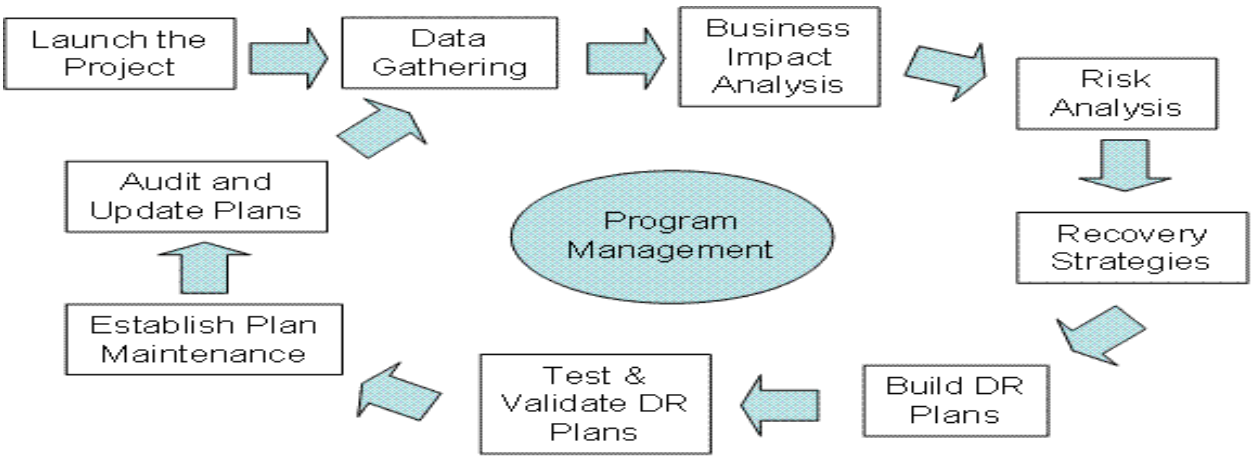

Figure 1.1: Key stages of disaster recovery plans

An Enterprise delegates a Disaster Recovery group inside the organization, which can effectively include in making the arrangement steps, actualizing and keeping up the arrangement (Milap, 2014). As a need, organizations associations make DRP formats as a reason for creating Disaster Recovery gets ready for the organization.

Hazard can never be disposed of; however it can be limited by the utilization of IT security controls. The decision with respect to what level of hazard will be known will be founded on administration survey of the identified IT security controls expected to mitigate the hazard against the potential effect of affecting those controls on accessibleassets and framework operations (SANS Institute 2007). The Risk Assessment recognizes the present level of hazard for the application and gives risk mitigation suggestions to management survey. The Risk

Assessment acts as the important get to control work for a few basic applications and the loss of framework accessibility as well as honesty that could devastatingly affect the association's central goal. The sympathy level of the framework and of the data put away inside, handled by, or transmitted by the framework mirrors theestimation of the framework to the organization Theaffectability level has been useas the center for inciting the important IT security controls for the framework (NIST Special Publication 800-37 2010-2014).

1.1 Thesis Problem

The problem of this research is to distinguishing the huge risks that are available in an association and how best we can arrange, organize and kill danger that could upset business congruity. (ISO17799) Some of the dangers are:

A) Natural Threats: A characteristic procedure can bring about death toll or property harm most likely prompt financial harm that could put the nation in a genuine subsidence (earth shudder in Nepal 2015) a portion of the common dangers are: Earthquakes, Floods, tornadoes, avalanches, torrential slides, electrical tempests, and such different events.
B) Human Threats: Events that areeither empowered by or brought on by people, for example, unexpected acts, Workers Health issue (incidental information passage) or consider activities (organize based assaults, pernicious programming transfer, unapproved access to classified data).
C) Environmental and Physical Threats: Long-term control disappointment, contamination, chemicals, fluid spillage. (Marinos, 2015 ENISA), and (Benjamin, 2012).

1.2 The Aim of the Thesis

The purpose of this study is to describe the risk assessment and disaster recovery plan in the field of information system technology in cloud migration data center (Bird, 2015). The aim is to identify threats and vulnerabilities applicable to information technology, toassess the probability that defenselessness can beabused. To evaluate theeffect related with these dangers and vulnerabilities, and to recognize the general hazard level, and how best cloud computing can be useefficiently in the data center era.

1.3 The Important of the Thesis

The importants of this thesis is to identify and evaluate different risk and vulnerabilities that could cause downtime for the organization directly and indirectly and the key drive of strategy of cloud migration of data center and how different cloud computing services can be used to give our customers good qualities and available service as at when needed.

1.4 Limitations of the Study

Inability to have access to some materials I needed. I had disappointments and delayed from different companies who I had consulted for risk assessment project materials to be carried out in their organization but all them back out due to theextends of reviewing their information out. I had some delayed from professors and expert of getting data and analysis.

1.5 Scope of the Study

The extent of this review is to assess dangers to Information Technology in the territories of administration, operational, and specialized controls. This hazard appraisal is constrained to System Boundary and included site visits to lead interviews at Location of Interviews and physical security surveys of locations where reviews took place.

- To distinguishes dangers and vulnerabilities pertinent to IT.
- To assess the probability that powerlessness can be abused.
- To evaluates the effect related with these dangers and vulnerabilities, and
- To distinguishes the general hazard level.

1.6 Overview of the Thesis

This research work describes IT vulnerabilities and related dangers. A risk and Vulnerabilities are not the same. Illustration (demonstration of psychological oppressor), A risk is a man or occasion that has the potential for influencing a profitable asset in a negative way. Vulnerability is that nature of an asset or its condition that enables the risk to be realized. (Catherine P. Cisco Press, 2013)

An armed bank robber is an example of a danger. A bank employee is a case of a significant asset that might be vulnerable during a bank robbery. Impenetrable glass between the robber and the bank teller denies the criminal the chance to shoot the teller. The danger stays present, yet one of its destructive impacts (a shot) has been mitigated by an insurance component (the glass).

In framework and system security, the dangers stay present however are mitigate through the best possible utilization of security elements and methodology. Mitigation is any push to keep the risk from having a negative eeffect, to restrict the harm where add up to avoidance is impractical, or to enhance the speed or adequacy of the recuperation exertion.

Equipment and programming frameworks and the information they process can be powerless against a wide assortment of dangers. The choice of security components and strategies must be construct with respect to general security targets as well as on the particular vulnerabilities of the framework being referred to in light of the dangers to which the framework is uncovered. It is conceivable toover-secure, which just squanders assets and burdens clients.

As should be obvious, there is a connection amongst risks and vulnerabilities. Here and there it is less demanding to look at every potential danger and decide the degree to which you are helpless (e.g. fire, flood, and earthquake). In different cases, it is simpler to search for potential vulnerabilities in view of no specific danger (e.g. dishonorable mounting of hardware, media disappointment, information dataentry mistake). With a specific end goal to land at a total risk assessment, both points of view must be inspected. Dangers and vulnerabilities are intermixed in the accompanying rundown and can bealluded to by and largeas potential "security concerns.

In this thesis, various threats, risks, and vulnerabilities have been discussed and how best they can beaddress toavoid down timeof any kind, the thesis also focused on data center migration in information systems technology.

Chapter one, explains the introduction of the study and enlightened more in details about various disasters and risk assessments and its tools. Chapter onealso displays problem of the thesis, theaim of the thesis, the limitation of the study, and its scope.

Chapter two, present overview of different research conducted on disasters recovery planning issues and solutions, enterprise architecture, Data protection in today Data Center, Risk assessment and management, and Cloud Computing.

Chapter three, explain the theoretical frame work of the study which consists of Risks standards and various kinds of Cloud Computing as services.

Chapter four, in this chapter service blueprints was defined and the model interactions and roles of Information risk management (IRM) and the concepts of App Suits was introduced, the

challenges identified and the key underlying principle that guide proposed solution. This chapter also addresses the four distinct of risk analysis and methodology as well as threats and vulnerabilities.

Chapter five, offer a model that focuses on how to combine both App of risk assessment and disaster recovery as oneapp by introducing requirements, presenting the specification and the design of the implementation of a decision support system for cloud migration. The migration support system aims to model and incorporate the identified risks and mitigation of emphasis on theextensibility of the system. This system is based on RESTful services and implementation in Java language.

Chapter six, draws conclusion and recommendation of future work.

CHAPTER TWO
RELATED RESEARCH

Literature Survey covers planning of risk assessment and disaster recovery scenario plans that domains and highlights industries best practices focusing on planning, strategy and correlating risk management and enterprise architecture leading to effective IT Governance. This research work focuses on Risk Assessment and Disaster Recovery Plan Scenario for medium and large scale IT Organization to improve visibility and provide Decision Support Metrics for DR Triage at Time of Disaster. The following sections review the published literature in respect to disaster management. The sections cover risk assessment, cloud Migration and disaster recovery concepts in the chronological order of Disaster Readiness, disaster relief, Disaster Recovery. Enterprise Architecture and Disaster Recovery planning, cloud computing

2.1 Disaster Readiness

Lately, expanded awareness has been paid to pre-disaster arrangements. Jackson and Paton (2002) battle that crucial to disaster preparation or readiness is the arranging and creating of fitting preparing courses of action. They propose that there are restricted open doors really gain the experience to manage catastrophes, so this choice can help prepare crisis laborers for emergency. Moe and Pathranarakul's (2006) examinations of the 2004 Asian tsunami that influenced Thailand uncovered that the nation was badly prepared for such an occasion. It was suspected that a disasters administration plan would have made a difference. Such an arrangement could incorporate the components of expectation, cautioning, mitigation and readiness, clear lines of specialist, viable coordinated effort, and training of groups in potential hazardous situations and a sufficient data base to work.

In addition, (Athukorala and Resosudarmo, 2005) investigations of the 2004 Asian tsunami as it influenced Indonesia and Sri Lanka observed, reaction frameworks to be lacking. Their assessment of the disaster administration process drove them to conclude that people in general ought to be better taught about safe security measures that can be taken amid a disaster. Taking after the September 11 fear based oppressor assaults in the United States, Perry (2003) recommends that much consideration was given to the territory of Incident Management Systems (IMS). These frameworks are a method for foreseeing conceivable disasters and after that getting

ready for the required assets that may be required in planning for possible disaster crises. Whybark (2007) likewise took a gander at how groups can be better arranged. He sees it in two ways, one that highlights the requirement for obliged things to be gained and put away in planning for when a disaster strikes. Alternate concentrates on making arrangements for the sourcing and dispersion of things amid the relief operations. Disaster readiness is accepted to be a basic piece of any disaster or crisis administration framework. This would incorporate arranged measures to be taken amid and after a catastrophe occasion. It ought to likewise incorporate setting up the fabricated condition for the conceivable results of disaster through construction standards and directions.

2.2 Disaster Relief

Disaster Relief is the principal reaction amid or after a disaster occurrence. Weigelt and Klein (1991), propose that once a disaster has struck we can't anticipate that everything will be found in its typical setting. Actually, they advances that as well as could be expected seek after is some type of "controlled turmoil". They likewise contend that we can't permit the ethos of goodwill and great expectations to force us through disaster relief circumstances. These occasions must have fitting arranging and administration. Yi and Kumar (2007), battle that there are the two noteworthy exercises that element in a disaster reaction. These are clearing of the influenced and coordination bolster. Their view is that clearings are the underlying reaction to expel individuals from a position of mischief or peril. Coordination support is what is required in the time after the underlying calamity occurrence to help survivors that are still inside the catastrophe zone. This help can be as nourishment, asylum, pharmaceutical and getting the injured to healing facility. Kovacs and Spens (2007) depict strategic support as far as compassionate coordination. They consider it to be an umbrella term for different disasters operations. They say it covers the underlying reaction and also persistent support for influenced locales.

In 2012, when Hurricane Sandy crushed the northeastern shore of the United States, Rx Response, now social insurance prepared now, kept crisis responders polished on the status of the biopharmaceutical inventory network. Rx Response's Rx Open instrument was conveyed in 11 states and the District of Columbia, helping casualties and evacuees who expected to fill or re-fill their medicines to find open drug stores. Rx Response likewise helped crisis responders with basic data on the difficulties confronting production network accomplices identifying with

power, fuel and transportation issues. Moreover, PhRMA and its part organizations coordinated representative gifts toward help endeavors.

Figure 2.1: Disaster relief, (Staff, 2012)

2:3 Disaster Recovery

Randy R. Rapp 2011 perspectives of disaster recovery as a blend of rebuilding and reproduction, reclamation alludes to repairing existing structures to their pre-disaster state while remaking is revamping from new. It is the entirety of these two exercises that place influenced areas headed for recovery. Buckle and Coles (2004) propose that successful recovery can just happen if the entire faculty works in behind the exertion. Nonetheless, the staff must have the limit and learning to embrace the works. It is expressed that as of late disaster administration is not seen as much as dealing with the peril but rather as dealing with the dangers included (Baradan, B. 2006).

2.4 Enterprise Architecture and Disaster Recovery Planning

This report underlines the relationship of IT Disaster Recovery Planning (DRP) and Enterprise design (ED) as incorporated exercises inside an organization by (David Rudawitz, Enterprise IT Solutions, (LLC) November 2003) The review outlined a sensible strategy used to comprehend an organization as a framework contained procedures and assignments and afterward extends this to an approach of making complete endeavor engineering. With this approach, an organization can make an a great deal more concise IT disaster recovery arrange for that is firmly combined

with both the business and IT, accordingly boosting the feasible for an effective recovery from disaster or business intrusion.

2.5 Data Protection Strategies in Today's Data Center

The paper discusses how a company could spend far less on data protection and yet protect its data better and efficiently than spending more and waste of time to protect its data. It lists out natures of failures, and talks about how to restore, recover and overcome after a Disaster Event. The document discusses how companies spend beyond budget on data recovery by using incompatible tools and often ones that provide more functionality than required per the business requirements. (Curtis, 2012)

2.6 Disaster Recovery Issues and Solutions

In their study, authors discussed paper discusses RTO and RPO ranges for different Tiers of Recovery based on Type of Storage. (Hitachi Whitepaper, By Rose Linda R. Schulman, Sept 2004). Recovery Point Objective (RPO), and Recovery Time Objective (RTO) alongside their related expenses, is critical criteria while assessing the correct solution.

- RTO portrays the time in which business capacities or applications must be reestablished incorporates time before disaster is recognized and time to perform errands.
- RPO portrays the indicate in time which information must be reestablished to effectively continue handling frequently considered as time between last reinforcement and when blackout happened.

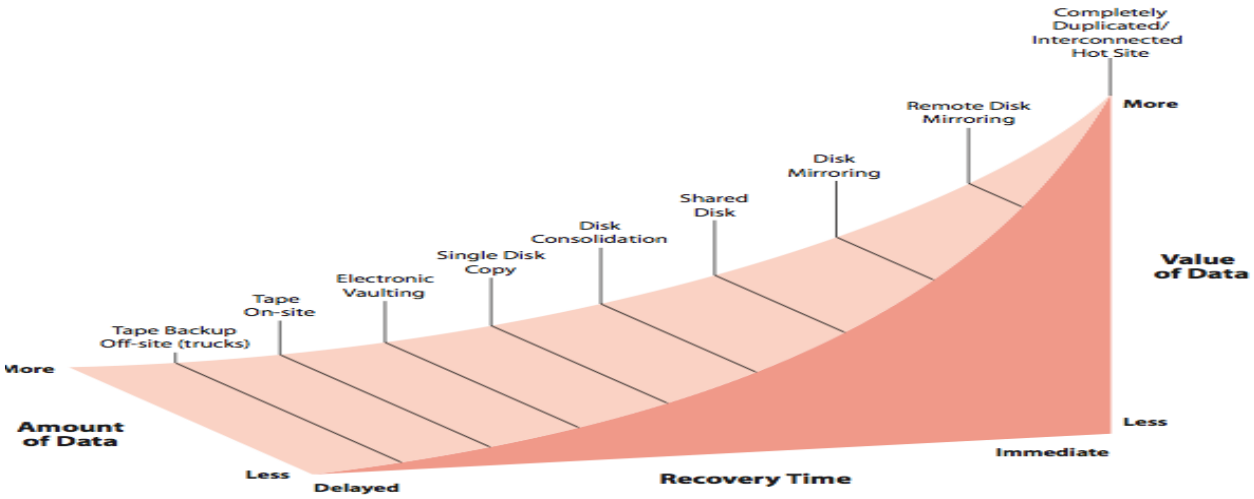

Figure 2.2: Data types and disaster recovery

A data audit is necessary to assess business criticality and cost to recover.Different types of data necessitate different levels of protection.

2.7 IT Governance and Enterprise Architecture: A Risk-Based Approach

This paper examines part of IT Governance, in their review, the authors talked about the Alignment of Strategy and Processes utilizing a Risk based approach. It gives a procedure that connections technology and business capacities, driven by the organization's main goal and needs, considering those responsible to a standard, for delivering the essential execution, to fulfill the internal and external partners. (By US Capitol Police James R. Getter, 40th Hawaii International Conference on System Sciences 2007)

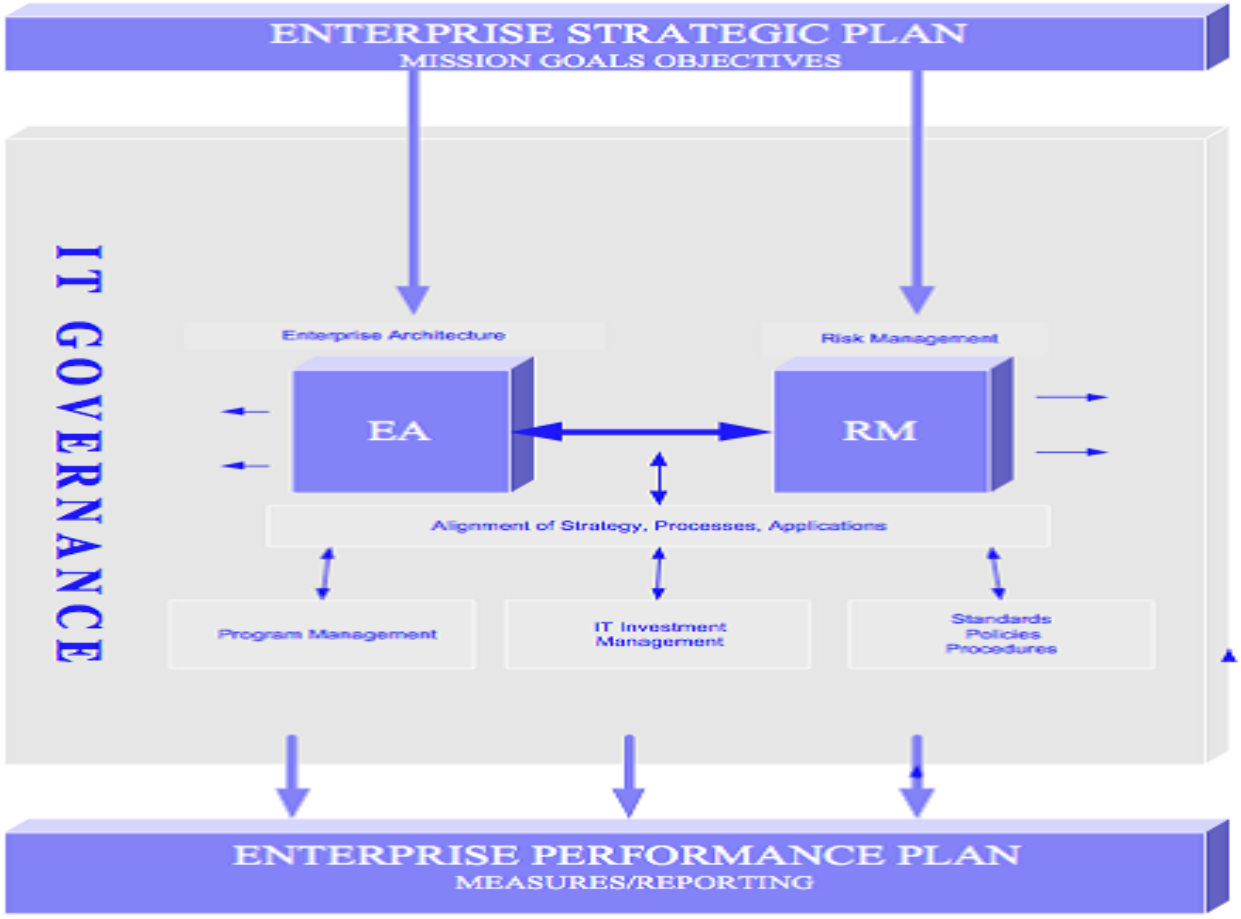

Figure 2.3: Enterprise framework

2.8 Risk Analysis and Management for Projects – (RAMP)

Hazard and vulnerability encompass each human action and impact all that we do. A later approach by the (Institution of Civil Engineers and Institute of Actuaries June, 2014 Charles Jensen) brought about a more far reaching procedure of Risk Analysis and Management for Projects (RAMP), intended to cover the total project lifecycle (referred to Tah and Carr, 2000). RAMP utilizes a multilevel breakdown structure. RAMP procedure includes principally four fundamental exercises. These exercises are in particular; prepare dispatch, hazard audit, risk administration and process closedown. lower level procedures separate these primary exercises assist. Establishment of Civil Engineers (ICE) and the Institute and Faculty of Actuaries (2014), these exercises are executed on various periods of a project. The first and last exercises in particular, handle dispatch and process shut down; each performed as soon as risk reviews are executed several times in essential times of a project and depending on these reviews risk management activities follow a continuous cycles. Process launch involves the supplementary documentation and preparation for objective definitions and scope development for risk analysis and management. This task is executed at the investment stage aiming to define general objective, scope and timing of investment. Temporary general methodology for hazard survey and administration exercises in the lifecycle of the investment, are stated. Scope of reviews and the stages where the reviews are required in what detail are considered at this stage (Jensen, 2014).

Definition of overall strategies for risk management and overview of project management involving the project stages are considered in this part of RAMP. People involvement has significant importance at this stage because responsibility definitions and life cycle planning of project is done at this stage.

Jense 2014, one of the hazard administration exercises or RAMP is hazard recognizable proof. The objective of this stage is to distinguish all critical hazard variables, sources and vulnerabilities related with each project objective. This stage begins with posting of dangers without the utilization of agendas or prompts. Taking after this, dangers are recorded in hazard enlist for consequent audit and examination, with a conditional sign of the importance of each hazard and interrelations in the middle. It is proposed a meeting to generate new ideas is completed for broad identification and amendment of dangers. After identification stage come the hazard examination, which points the evaluation of subjective and quantitative qualities for

probability of dangers per unit of time, potential results of dangers, and timing of the hazard's effect and the acknowledgment score, by joining the probability with the outcome utilizing risk assessment tables. It is essential to begin with a characteristic or helpful reason for estimation, and connection this to an existence lifecycle estimate. In the event that there is a scope of conceivable qualities, it might be worthy, to speak to the range by its mid-point or normal esteem. In the event that a hazard is identified with at least one different risk as in they share normal causes or for different reasons the event of one influences the probability of another-the related dangers ought to be assessed together. The subsequent assessment of each hazard or gathering of related dangers ought to be entered in the hazard enlist.

Chapman, C.B. and Ward, S.C, 2003. The essentialness of dangers ought to be looked into and afterward they ought to be renamed into the classes of centrality. For dangers, which are 'presumably immaterial', the choice must be made regarding whether they can be overlooked. Mitigating dangers, or diminishing their unfavorable effects, is at the heart of the successful administration of hazard. Shockingly, in business exercises risk mitigation is in some cases embraced just at a somewhat shallow level. On the off risk that more consideration were paid to it, less business exercises would end in misfortune. It is not adequate just to 'take an edge' for hazard, since this outcomes in little hazard mitigation being finished. In the event that actualized effectively a fruitful hazard relief system ought to decrease any antagonistic varieties in the money related comes back from a project. Be that as it may, hazard mitigation itself, since it includes coordinate costs like expanded capital use or the installment of protection premiums, may decrease the normal general money related comes back from a project; this is frequently an impeccably worthy result, given the hazard avoidance of numerous speculators and banks. Hazard relief ought to cover all periods of a project from origin to shut down. Dangers can be managed inside the setting of a hazard administration procedure in four fundamental ways.

- Reduced or wiped out
- Transferred
- Avoided
- Absorbed or pooled.

There is likewise the subject of whether it merits doing exploration to diminish instability. The project proposition on which the choice to continue or not will be based ought to unite a

depiction of the project and its gauge a portrayal of the most critical dangers and how it is proposed to alleviate them. A representation of the residual dangers and the impact they will have on net present esteem (NPV) if there are noteworthy option alternatives, a suggestion on which ought to be Chosen a proposal on whether the project ought to go before matters outside the extent of RAMP. The last stage is to acquire formal approval from the customer and whatever other stakeholders for continuing with the project. The managers will assess both the arithmetical outcomes acquired and a scope of elusive elements.

The key undertaking at this phase of RAMP is the observing of dangers incorporated into the lingering hazard examination, risk mitigation system and the hazard reaction arrange. Different dangers additionally should be observed frequently incorporating those in the rest of the phases of the project life cycle not just the dangers happening in the present stage. Any critical changes in hazard or new dangers ought to be accounted for and evaluated quickly. Customary observing of dangers can be attempted by contemplating occasions, circumstances or changes (once in a while called 'patterns'), which could conceivably influence dangers amid the ordinary administration and advance of a investment. Institute of Civil Engineers (ICE) and the Institute of Actuaries (2014), these patterns must be efficiently recognized, examined and observed all the time by investigating reports, letters, and notes on visits, gatherings and phone discussions. The outcomes are entered in pattern plans. Preferably, these ought to be considered at general advance gatherings including key individuals from the administration group. At long last, the major benefits of the investment regardless of whether it is beneficial, ought to be persistently evaluated and a hazard audit set close by when occasions happen which seem to have essentially adjusted the hazard profile of the project.

Toward the finish of the investment life cycle, or on earlier end of the project, a review survey will be made of the investment and of the commitment and viability of the RAMP procedure itself as connected to the project. The risk procedure administrator, in conjunction with the customer's illustrative, will initially assess the execution of the project, contrasting its outcomes and the first targets. Utilizing hazard survey reports and the hazard journal, an assessment will be made of the risks and effects, which happened in examination with those expected, highlighting dangers which were not predicted or terribly erred. The hazard procedure supervisor will then fundamentally survey the adequacy of the procedure and the way in which it was directed for these investments, drawing lessons from the issues experienced and proposing upgrades for

future projects. The aftereffects of the audit will be recorded in a RAMP closedown report, which can be effortlessly alluded to for future projects. Duplicates of the report ought to be flowed to all gatherings included and after that closed down by each gathering as a concurred record of occasions.

A few tasks will be ended when the underlying danger survey has been finished, in light of the fact that the hazard remunerate proportion is not esteemed adequately appealing and different undertakings will be ended before the finish of their arranged life cycle as a result of antagonistic improvements. The generation of a RAMP closedown report as a guide for different projects is probably going to be especially important in these conditions on the grounds that the most basic occasions in the historical backdrop of the venture will have happened as of late. The PRAM and RAMP approaches endeavor to beat the casualness of most hazard administration endeavors.

2.9 Risk Management

Risk management envelops three procedures: risk assessment, danger mitigation and evaluation. Risk management is the procedure that enables IT supervisors to adjust the operational and financial expenses of defensive measures and accomplish picks up in mission ability by securing the IT frameworks and information that bolster their organizations' missions. This procedure is not one of a kind to the IT condition; in reality it invades basic leadership in every aspect of our day by day lives. Take the instance of home security, for instance. Many individuals choose to have home security frameworks introduced and pay a month to month charge to a specialist organization to have these frameworks observed for the better insurance of their property. Probably, the property holders have measured the cost of framework establishment and checking against the estimation of their family unit merchandise and their family's security, an essential "mission" requires. The leader of a hierarchical unit must guarantee that the organization has the abilities expected to fulfill its main goal. These mission proprietors must decide the security abilities that their IT frameworks must need to give the desirable level of mission support even with true dangers. Most organizations have tight spending plans for IT security; in this way, IT security spending must be assessed as altogether as other administration choices. A very much organized hazard administration procedure, when utilized viably, can help administration distinguish fitting controls for giving the mission-fundamental security capacities.

According to the ISO 31000 (2009), risk is defined as the effect of uncertainty on objectives, where uncertainties refer to the events, which may happen or not, and caused, by lack of information. Risks can lead to a series of positive or negative concerns in terms of economic concert, professional reputation, safety, compliance, strategy, as well as environmental and societal outcomes. Thus, risk management is even more important to organizations or enterprises in modern society. Risk management is a critical part of any strategic management. It involves identifying, analyzing, assessing and taking steps to reduce or eliminate the loss towards an organization or individual. The application of risk management utilizes many tools and techniques to manage various risks. At the meanwhile, several risk management standards have been developed by different organizations, such as the National Institute of Standards and Technology, the Project Management Institute and ISO standards as well. ISO 31000, Risk management Principles and guidelines, is a standard of risk management codified by the International Organization for Standardization in 2009. It gives standards, structure and a procedure for overseeing dangers and can be connected for any open, private or group enterprise, affiliation, gathering or person. In this manner, ISO 31000 is not expected to be particular to any industry or organization, rather to give a typical worldview and rules to all exercises worried with hazard administration.

CHAPTER THREE
THEORETICAL FRAME WORK

3.1 Overview

This chapter provide over views of the detailed risk analysis of threat, vulnerabilities, and risks. Analyzed how best cloud computing can help fashion data center in terms of maintenance and best practice, cost effective management, performance, efficiency and availability, in the field of information system technology. This chapter also focuses on Data Center Migration to the Cloud and the various risk involved in data center and migration.

Identification of Assets: Resources within the system boundary that require protection according by the 2013 modification of (ISO 27001) enables you to recognize dangers utilizing any technique you like, however the old approach characterized by the old version of (ISO 27001) which requires IDs of dangers, vulnerabilities and resources. The goal of asset identification is to pro-actively collect all necessary information about an organization's assets that can be useful in reacting to a threat heartrending that asset.

Identification of Threat Sources and Vulnerability: Limitation in the framework plan, framework security techniques, execution, and inner controls that could be misused by approved administrators or impostor.

Identification of Threat: Known and anticipated dangers that are identified with the framework under survey.

3.2. Record Creation Process

This section explains the process and the way of how the new catalogue of risk identification is formed. The risk catalogue is founded on the risk description standard defined by IRM and applies it to identify the risks of cloud migration by referring to a large number of academic papers and reports. The most heuristic reference of this catalogue is the method of identifying risks and the spreadsheet (available from PlanForCloud.com) by Khajeh-Hosseini, 2012.

3.2.1 Process of Risk Identification

To make the new inventory of hazard ID includes four noteworthy strides, which is delineated in Figure 3.1:

- Make a reasonable comprehension of the spreadsheet of hazard recognizable proof by Khajeh-Hosseini 2012 and break down each hazard portrayal to confirm whether it happens to be sure by cloud relocation or examine whether it can be converged with different dangers.
- Add dangers which are excluded in this spreadsheet by alluding to other related works.
- Collect and rename every one of the dangers with five new classes (Financial, Compliance, Knowledge Management, and Operational and Strategic).
- Adapt every one of these dangers into IRM layout with including all data required.

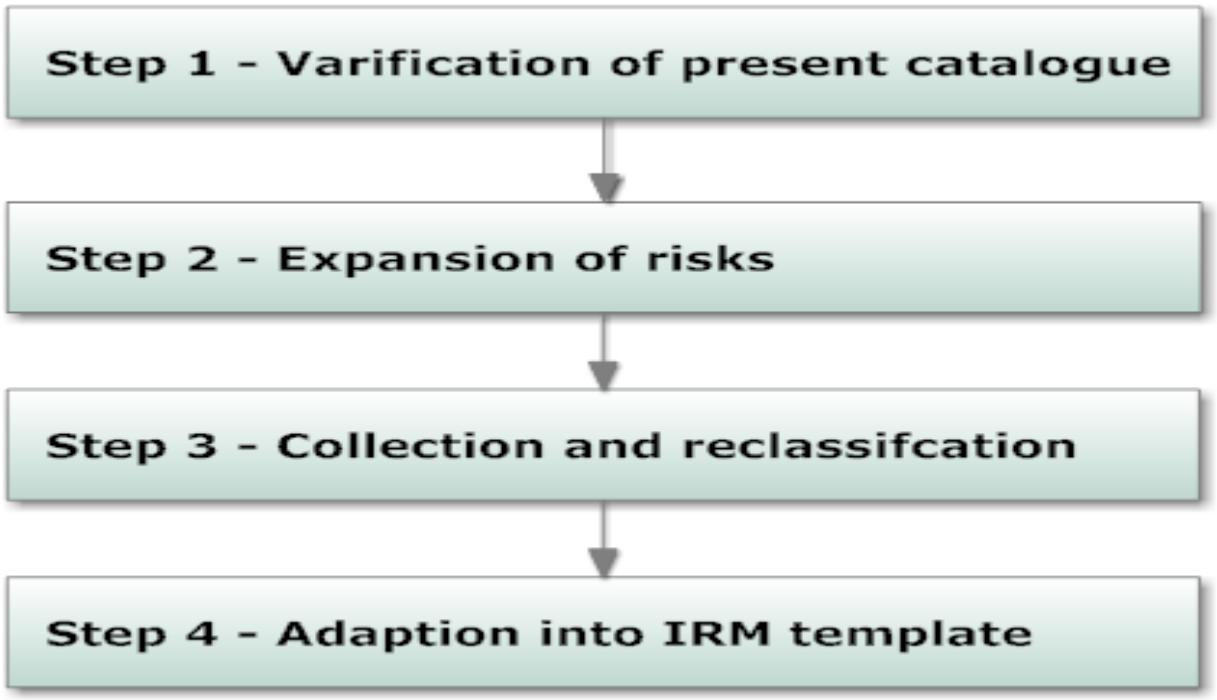

Figure 3.1: Four steps of risk identification

Firstly, all the hazard Identification by Khajeh-Hosseini is utilized as an establishment of our new hazard record. This hazard record is accessible from PlanForCloud.com as a Google Docs spreadsheet. This spreadsheet has two tabs, one for hazard and one for advantages, which means to bolster risk management and guarantee that the managers can make expert trade between the advantages and dangers of utilizing the cloud. In correlation with the 5 classifications in hazard sort (Compliance, Financial, Knowledge Management, Operational and Strategic) characterized by IRM, 39 risks are arranged additionally in five classes (Organizational, Legal, Security, Technically and financially) with their portrayals and relief approaches in this spreadsheet. After

a careful examination of this work a large portion of the leaving risks are stayed since they are ended up being happening amid cloud movement. For instance, R1 characterizes a circumstance in which the clients can buy processing assets utilizing their own charge cards without express endorsement from focal IT division. This may bring about loss of administration or control over assets in both physical and administrative angles, which is additionally depicted in numerous different records, for example, the work from J. Dibbern 2002. We keep up this hazard with an appropriate name in our inventory and arrange it later into the sort Strategic. A few dangers like R38, which portrays wild wellsprings of information exchange deferral or bottlenecks, are excluded because of absences of reference in different archives. However there are additionally a few dangers that can be developed to other hazard. For instance R8 clarifies a comparable setting of danger of loss of administration and control over frameworks like R1, just in the part of administration quality. So we mastermind these two dangers with one ID in the new index.

After redesign of present spreadsheet, a few dangers ought to be additionally considered in the hazard accumulation in step 2. For instance, there are many articles and reports specify that nature catastrophe could be a danger for distributed computing. Tropical storms, seismic tremors or it might devastate the equipment or database of cloud supplier and the client's information could be harmed or lost, as depicted in such report by ENISA 2012. Be that as it may, there is no relating depiction in Khajeh-Hosseini's spreadsheet. Hence we include this into the new hazard list too. In step 3, we gather every one of the risks found and rename them with new classes characterized by IRM hazard standard. As indicated by the Khajeh-Hosseini's spreadsheet, risks are grouped in 5 classes with hierarchical, lawful, specialized, security and money related. After investigation we discovered that the dangers in Financial allude to inadequate administration and control of the expenses of an association and different dangers in money related issues, for example, credit, remote trade rates and so forth. These dangers that are in the first classification budgetary ought to be kept up with similar classifications name, for example, R34 in the spreadsheet, which is related to R8 over move" in the new list. However a few dangers ought to be independently consigned, on the grounds that these could occur in period of arranging when the administration group settled on a wrong choice on cloud relocation. Varying from other authoritative dangers, these dangers can lead a progression of negative outcomes with tremendous misfortune.

Thusly another class in key is on request and certain hazard, for example, R1 by Khajeh-Hosseini is relating to R39 with Strategic in our list. After improvement of present spreadsheet, a few dangers ought to be likewise considered in the hazard gathering in step 2. For instance, there are many articles and reports say that nature disaster could be a danger for distributed computing. Typhoons, seismic tremors or it might decimate the equipment or database of cloud supplier and the client's information could be harmed or lost, as depicted in such report by ENISA 2012. Be that as it may, there is no comparing portrayal in Khajeh-Hosseini's spreadsheet. In this way we include this into the new hazard inventory also.

In step 3, we gather every one of the dangers found and rename them with new classifications characterized by IRM risk standard. As indicated by the Khajeh-Hosseini's spreadsheet, risks are grouped in 5 classifications with hierarchical, legitimate, specialized, and security and money related. After examination we discovered that the risks in Financial allude to inadequate administration and control of the expenses of an association and different dangers in money related issues, for example, credit, remote trade rates and so forth. These dangers that are in the first class monetary ought to be kept up with a similar classification name, for example, R34 in the spreadsheet, which is related to R8 \over move" in the new index. However a few dangers ought to be independently consigned, on the grounds that these could occur in period of arranging when the administration group settled on a wrong choice on cloud relocation. Contrasting from other hierarchical dangers, these dangers can lead a progression of negative outcomes with colossal misfortune. Consequently another classification in key is on request and certain hazard, for example, R1 by Khajeh-Hosseini is relating to R39 with Strategic in our inventory. Also there are a few dangers that the association is regular gone up against keeping in mind the end goal to accomplishing the vital objective. These ought to likewise be sorted into another sort named Operational from those hierarchical dangers, e.g. the previous R11 in authoritative, which depict a circumstance in imperviousness to change coming about because of hierarchical governmental issues and changes of working way, is currently related to R32 in Operational.

Subsequent to gathering every one of the risks that are from the first authoritative from spreadsheet into vital and operational, we found that some legitimate dangers, for example, R16 from the spreadsheet, which is resistance with information privacy controls, ought to be re-ordered in Compliance as indicated by IRM standard. Additionally, those dangers of security in

previous list depict certain situations in which information might be debilitated because of specialized issues, for example, program vulnerabilities in R25 or capture attempt of API messages in travel in R23. Since Knowledge Management by IRM is characterized to concern all the learning and specialized issues, we sort the dangers of security into this sort. Absolutely all the specialized hazard like R28 which is the terrible management execution, ought to be likewise in ordered in knowledge management, since it alludes to ineffectual administration and control of the learning assets and innovations.

3.2.2 Risk Description Standard

According to the definition by IRM, identified risks can be displayed in a structured format risk description table, as presented in Table 3.1. This table can be used to fastforward the description and evaluation of risks. Well planned risk description structure should contain sufficient information about the risks name, reference, how it could happen, stakeholders and their expectations, probability of its occurrence, influence and consequence when it happens, and some treatments or improvement should also be involved in order to eliminate risks or mitigate the impacts. With all these information a relative comprehensive understanding about risks would be obtained, which could happen in the whole business process. This work is based on the general risk description standard from IRM and has applied it into the risk identification and assessment in cloud.

Table 3.1: Risk Description by IRM (Institute of Risk Management, London, 2002)

S/N	LIST OF RISK	DISCRIPTION OF RISK
1	The extension and documentation of hazard	Qualitative report of occasions, their size sort number and conditions
2	Typre of hazard	It could be operational, budgetary, information or lack of involvement and key. or passivity and strategic.
3	Key Holders	Key holders and their prospects

4	Condition or hazard	Probabililty and centrality of the hazard
5	Risk Tolerance and Craving	Probability size of the potential misfortunes and increases goals for the control of the hazard and coveted level of execution. Misfortune potential and money related effect of hazard esteem
6	Risk administration and control method	The principle essential points is assess how hazard is as of now oversaw and the level of trust in the current control distinguishing proof of conventions for checking and audit
7	Possible action for development	Approvals to lessen hazard changes
8	Strategy and approach advancements	Identification of capacity in charge of creating methodology and strategy

3.3 Integration of Risk Management into SDLC

Programming advancement process or the Software Development Life Cycle (SDLC) is a structure unnatural on the improvement of a product framework. As indicated by this structure the product advancement process includes five distinct stages: Requirements Analysis and Definition, Design, Implementation and Unit Testing, Integration and System Testing and the Operation and Maintenance stage (Khdour and Hijazi, 2012).

Hazard elements required in each of these stages undermine extend achievement. This brings up issue about new enhanced hazard administration instruments. Numerous definitions, methodologies and systems exist for programming venture chance administration in the writing. Most prompt the use of the arrangement of standards, practices, methodology, strategies and devices gone for recognizing, breaking down and dealing with hazard figures through the SDLC before they advance into genuine issues that adversely influence the project improvement prepare and impede the effective finishing of the project. Risk administration can be either responsive or proactive. In the responsive methodologies, dangers are not relieved till their event, while in the proactive we attempt to evade the event of dangers. Plainly, it is ideal to maintain a

strategic distance from dangers as opposed to repairing from their results (Singh and Goel, 2007).

A preventive hazard administration technique intends to continue into the advancement procedure exercises and the SDLC stages and hazard control methodologies with an eye towards the recognized dangers and keeping them from being appeared. A hazard administration technique is a control movement that goes for managing a particular hazard factor(s). Not all hazard elements are controllable (Zardari, 2009), a few elements may be out of project managers control. Any product hazard element can be either avoidable or non-avoidable. For the avoidable hazard elements alleviation procedures are concocted and proposed to manage chances before they develop into genuine issues. Else, if the dangers are non-avoidable, or if the dangers have developed into genuine issues, then emergency courses of action need to happen with a specific end goal to repair from the event of these dangers. A moderation system goes for either evading the event of a hazard, or decreasing its belongings if there should arise an occurrence of event. This decrease can be accomplished by diminishing either the seriousness of the hazard or its probability. Either the moderation procedures or the alternate courses of action must be arranged ahead of time (Shahzad and Safvi, 2008). At the end of the day, we should not hold up till the event of the risks, then begin to consider and outline systems. Plainly, applying an alleviation technique is superior to anything leading an alternate course of action, since it is less expensive and simpler than repairing from hazard.

Constraining negative impact on the business prerequisite for exhaustive introduce in fundamental authority are the basic objectives of the association put into operation a risk organization prepare for their IT structures (NIST Special Publication 800-12, 1995). Convincing threat organization must be totally consolidated into the SDLC. Additionally, the IT system's SDLC has five phases: begin, headway or getting, utilization, operation or support, and exchange. Once in a while, IT system may have a couple of these phases meanwhile. Regardless, the danger organization framework is the same paying little regard to the Software Development LifeCycle arrange in which assessment reality drove. Hazard organization is a precise system that can be executed in the midst of each huge time of the SDLC. In table 2.1 delineates the characteristics of SDLC Phases Features of individually SDLC, arrange demonstrates how the danger organization, can be executed in keeping up each stage.

Table 3.2: Integration of Risk Management into the SDLC

ACTIVITIES	SUPPORT FROM RISK MANAGAMENT	
Stage One Initiation	The requirement for an IT framework is verbalized and the points and the extent of the IT framework is reported	Identified dangers are utilized to bolster the advancement of the framework necessities, including security prerequisites, and a security model of operations (methodology)
Stage Two Development or Acquisition	The IT framework is planned, bought, customized, created, or generally built.	The dangers distinguished amid this stage can be utilized to bolster the security investigations of the IT framework that may direct to engineering and configuration exchange offs amid framework advancement
Stage 3 Implementation	The framework security elements ought to be arranged, empowered, tried, and checked	The hazard administration handle bolsters the evaluation of the framework usage against its necessities and inside its demonstrated operational condition. Choices with respect to dangers recognized must be made preceding framework operatio
Stage four Operation or Maintenance	The framework plays out its capacities. Regularly the framework is being adjusted on a continuous premise through the expansion of equipment and programming and by changes to hierarchical procedures,	Risk administration exercises are performed for occasional framework reauthorization (or reaccreditation) or at whatever point real changes are made to an IT framework in its operational, creation condition (e.g., new framework interfaces)

	approaches, and techniques	
Stage five Disposal	This stage may include the mien of data, equipment, and programming. Exercises may incorporate moving, chronicling, disposing of, or obliterating data and sterilizing the equipment and programming	Risk administration exercises are performed for framework segments that will be discarded or supplanted to guarantee that the equipment and programming are legitimately discarded, that lingering information is suitably taken care of, and that framework relocation is led in a protected and deliberate way

3.4 Risk Assessment

Risk assessment is the essential methodology in the risk organization technique. Affiliations use risk examination to choose the level of the potential risk and the danger related with an IT structure every through it SDLC. The yield of this system perceives reasonable controls for diminishing or getting rid of peril in the midst of the danger mitigation plan, as analyzed in Section 4. Danger is a segment of the likelihood of a given hazard source's honing a particular potential helplessness, and the consequent impact of that ominous event on the affiliation.

To choose the likelihood of a future hostile event, threats to an IT system must be destitute down in conjunction with the potential vulnerabilities and the controls set up for the IT structure. Influence implies the degree of naughtiness that could be brought on by a peril's action of vulnerability. The level of impact is managed by the potential mission impacts and therefore makes a relative motivating force for the IT assets and resources affected (e.g., the criticality and affectability of the IT system sections and data). The danger examination procedure joins nine fundamental steps, which are delineated in Sections 3.1 through 3.9.

Step 1. System Characterization (Section 3.1)

Step 2. Threat Identification (Section 3.2)

Step 3. Vulnerability Identification (Section 3.3)

Step 4 Control Analysis (Section 3.4)

Step 5 Likelihood Determinations (Section 3.5)

Step 6 Impact Analysis (Section 3.6)

Step 7 Risk Determinations (Section 3.7)

Step 8 Control Recommendations (Section 3.8)

Step 9 Results Documentation (Section 3.9)

The essential Steps of 2, 3, 4, and 6 can be appeared in parallel after Step 1 has been finished. Figure 3-1 portrays these means and the contributions to and yields from each progression.

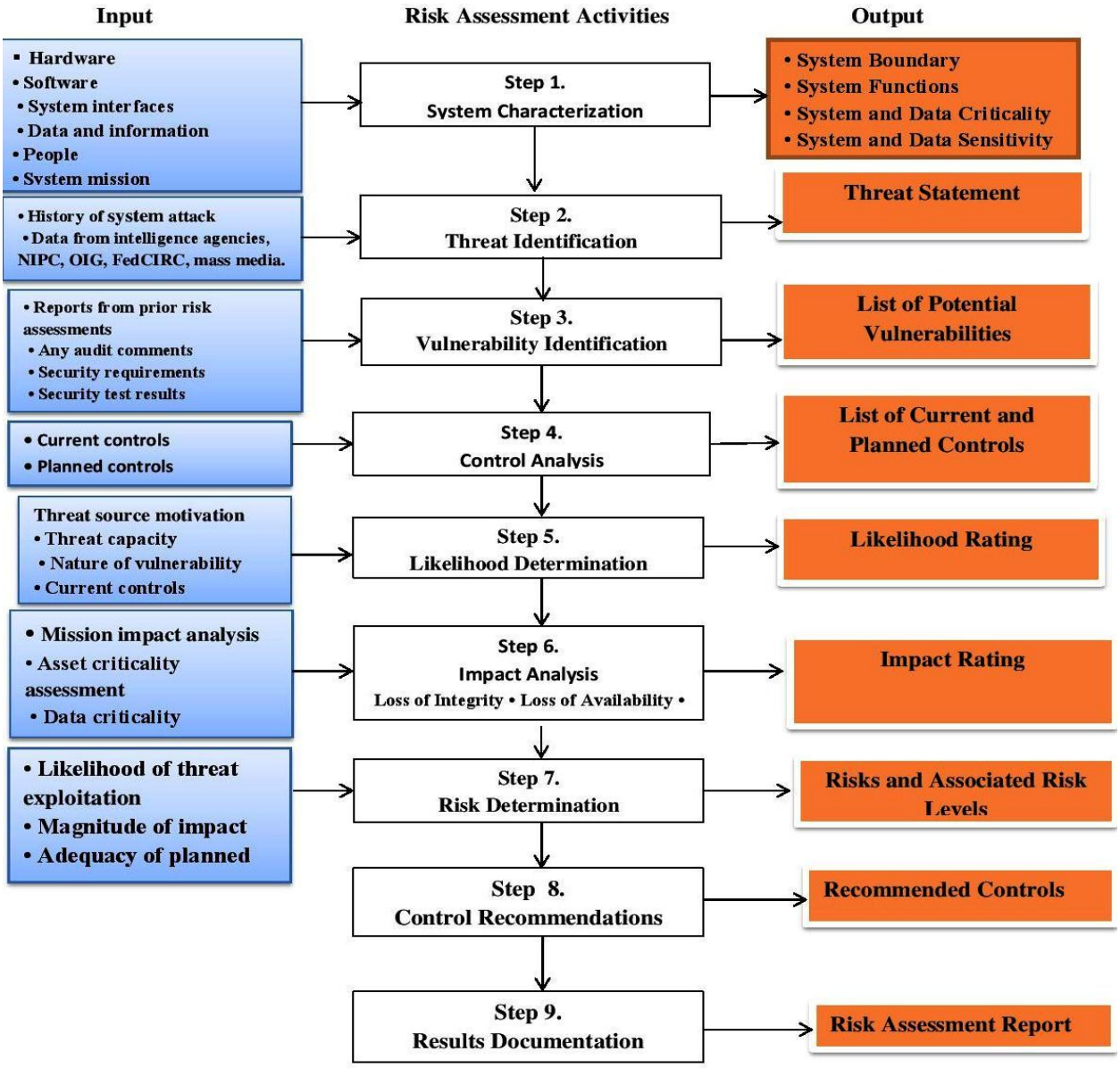

Figure 3.2: Risk assessment methodology flowcharts

3.4.1 External and Internal Factors

The dangers can come from anywhere because there are elements of both internal and external to the company. The Figure 3.3 outlines some particular risks and show in which territories they respond. These dangers can be isolated here into four sorts:

A) Financial Risks, which incorporate dangers from;

- Price (e.g. resource esteem, financing cost, remote trade or ware)
- Liquidity (e.g. income, call chance, open door cost)

- Credit
- Inflation or obtaining power
- Hedging or premise chance

3.4.2 Background

- Demographic and social patterns
- Technological development in industry
- Capital accessibility – administrative and political patterns

A) Operational Risks, which incorporate dangers from:

- Business operations (e.g. HR, item improvement, limit, effectiveness, item/benefit disappointment, channel administration, production network administration, business cyclicality).
- Empowerment (e.g. initiative, change status)
- Regulations
- Board organization
- Information innovation (e.g. significance, accessibility)
- Information or business revealing (e.g. planning and arranging, bookkeeping data, benefits finance, venture assessment, tax collection)

B) Hazard Risks, which incorporate dangers from:

- Natural or ecological harm – robbery and other wrongdoing, individual damage
- Business interference – ailment and handicap of representatives
- Liability claims
- Contracts issues.

C) Strategic Risks, which incorporate dangers from:

- Reputational harm (e.g. trademark or brand disintegration, extortion, ominous exposure)
- Competition
- Customer requests

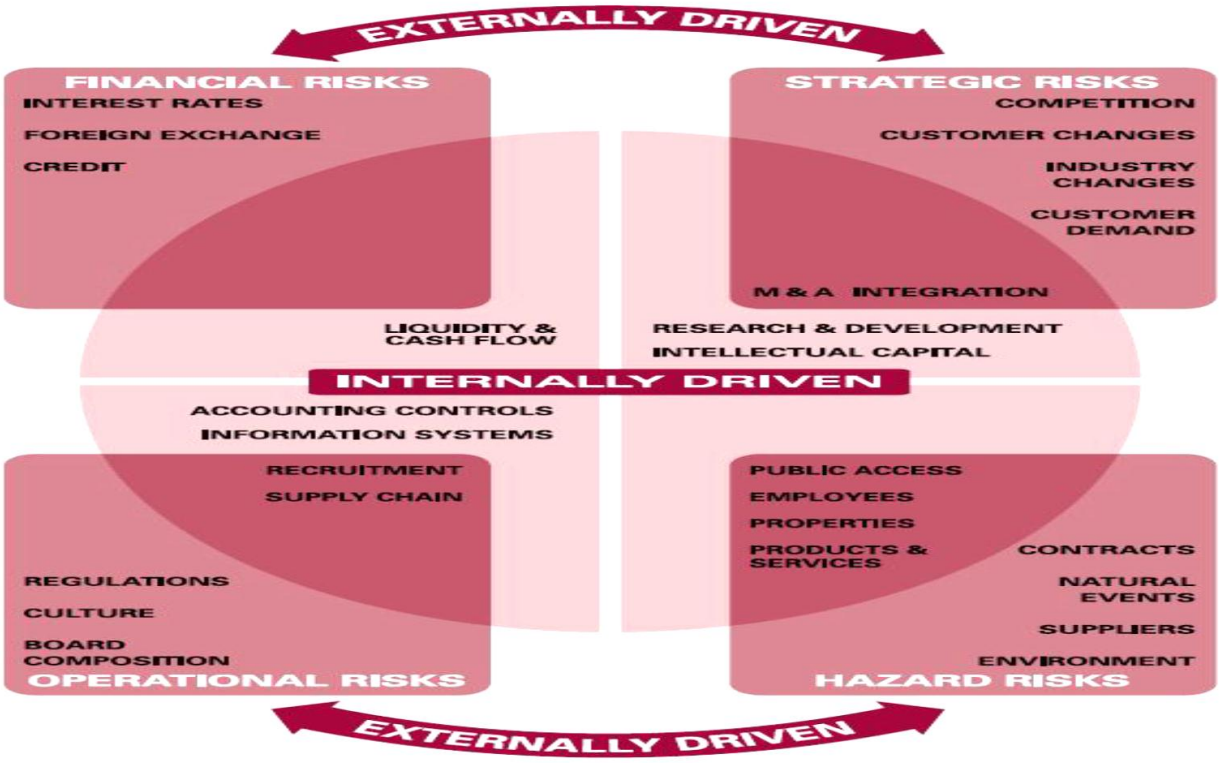

Figure 3.3: Drivers of key risks

3.5 Risk Assessment for Cloud Migration

The current improvement in cloud innovations and the increasing number of cloud users, organizations additionally need to stay aware of the present innovation to give genuine business solution. Moreover, expectations for development show huge advancements and usage of cloud computing services including that the distributed computing administrations advertise come to between $150 billion in 2014 and $222.5 billion in 2015. Cloud computing ends up noticeably one of the key innovations from the business point of view, that give genuine guarantee to business with genuine preferences in term of computational power and cost. Notwithstanding the advancement in cloud technologies and expanding number of cloud users, Cloud registering being a novel innovation begin new security hazards that should be evaluated and assessment. Therefore, evaluation of security dangers is fundamental, the conventional specialized strategy for hazard assessment which fixates on the advantages ought to offer route to the business, concentrated on the particular way of cloud computing and on the adjustments in technology that have another methods for noting cloud suppliers to convey their cloud buyers administrations.

3.6 Data Center Migration to Cloud

Moving IT frameworks and foundation to a private or open cloud can be a dampening challenge notwithstanding for the most experienced IT proficient. In the meantime, it gives an extraordinary chance to overhaul, reconsider, and enhance an association's IT engineering The drivers behind moving a server farm, or parts of a server farm, to the cloud are various they can by and large be partitioned into two classes: prerequisites and system (Tailor Bird Principal Architect – cloud arrangements at Nimbo).

- An organization’s present data center can at no time in the future bolster the requirement for development regarding current space, power and cooling.
- An organization’s present data center has an excessive number of single purposes of disappointment and the danger of blackouts.
- An organization’s rebuilding because of a merger or obtaining, making a need to discrete and additionally solidify server farms.
- An organization’s confronts the offer of a building, rental expenses, or increments in co-area costs.

Deliberately, Migrating Data focus to the cloud it help to diminish capital consumption and is one of the key drivers behind server farm cloud movement by utilizing cloud-based server farms, associations pay for the assets they expend and spare time and cash by expelling the need to purchase, introduce, arrange, and keep up a costly on-premises framework.

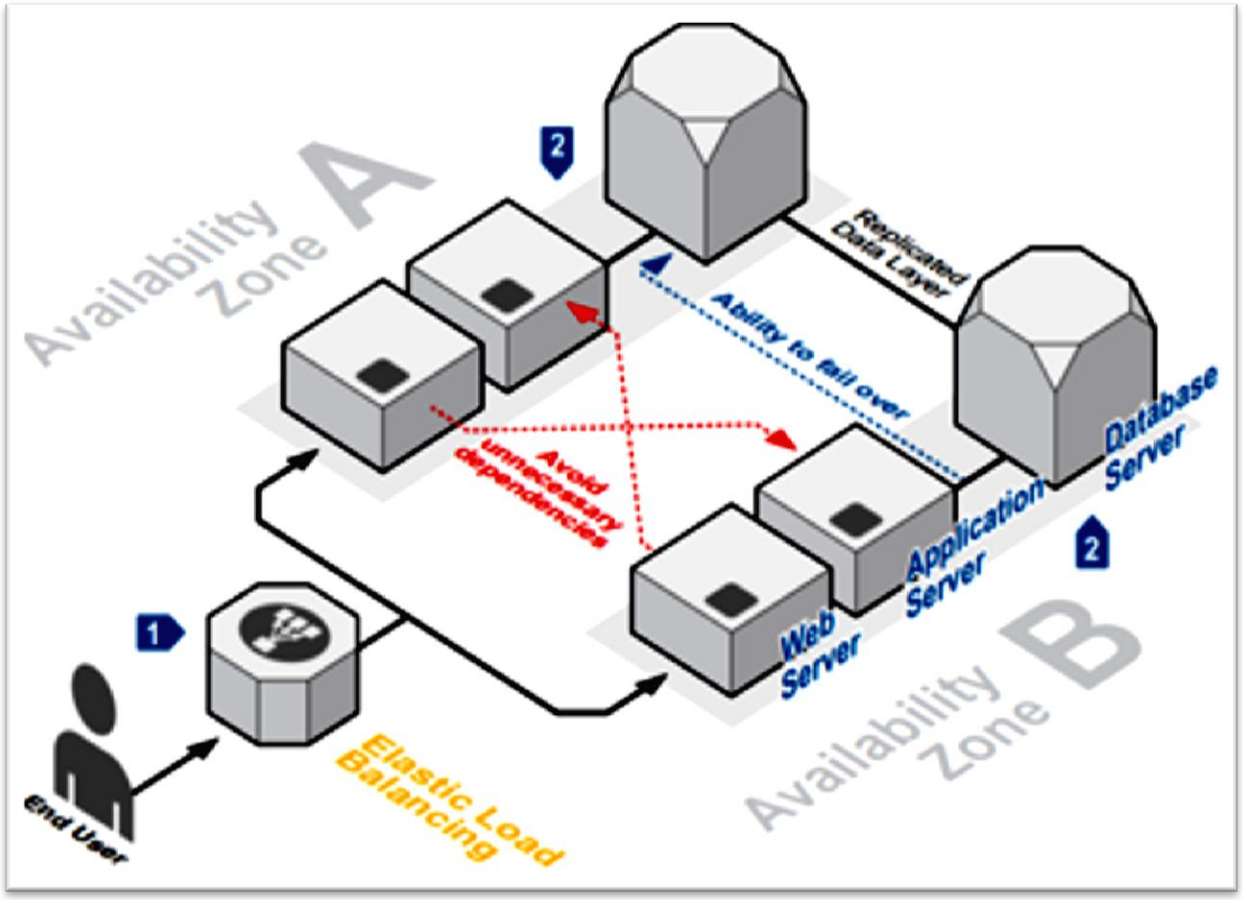

Figure 3.4: High availability and disaster recovery

3.7 Cloud Computing

Nowadays there is an new trend that more and more enterprises choose cloud computing for IT solutions. Cloud computing is a on-demand service model for IT provision, mostly based on virtualization and distributed computing technologies. Cloud computing is a sort of Internet-based computing that gives shared PC handling assets and information on the PCs and different gadgets on request. It is a model for empowering omnipresent, on-request access to a common pool of configurable processing assets (e.g., PC systems, servers, stockpiling, applications and administrations), by (Hassan, Qusay 2015) which can be quickly provisioned and discharged with insignificant administration exertion. cloud computing and capacity arrangements furnish clients and ventures with different abilities to store and process their information in either exclusive, or third party data centers that might be situated a long way from the user–ranging in separation from over a city to over the world. Cloud computing depends on sharing of assets to accomplish lucidness and economy of scale, like a utility or (like the power framework) over a power arrange by (Peter M and Timothy G, 2011).

Advocates guarantee that cloud computing enables organizations to maintain a strategic distance from in advance infrastructures costs (e.g., buying servers). Also, it empowers associations to concentrate on their center organizations as opposed to investing energy and cash on PC framework by M. Haghighat, S. Zonouz, and M. Abdel-Mottaleb (2015). Advocates additionally guarantee that cloud computing enables undertakings to get their applications up and running quicker, with enhanced sensibility and less upkeep, and empowers data innovation (IT) groups to all the more quickly alter assets to meet fluctuating and unusual business request. Baburajan .R, (2011) Cloud suppliers normally utilize a "pay as you go" show. This will prompt suddenly high charges if heads don't adjust to the cloud evaluating model.

In 2009, the accessibility of high-limit systems, minimal effort PCs and capacity gadgets and the across the board reception of equipment virtualization, benefit situated design, and autonomic and utility processing prompted a development in cloud computing. Companies can scale up as registering needs increment and afterward downsize again as requests reduction. In 2013, it was accounted for that distributed computing had turned into a profoundly requested administration or utility because of the upsides of high processing power, shabby cost of administrations, elite, versatility, openness and in addition accessibility. Some cloud sellers are encountering development rates of half every year (Dealey, C 2013), however being still in a phase of outset, it has pitfalls that should be routed to make cloud computing administrations more solid and easy to use, (Tech Republic 2015). According to the investigation from International Data Corporation (IDC), the worldwide prediction for clouds benefits in 2013 sums to $44.2 billion, with the European market cluster from 971 million in 2008 to 6.005 billion in 2013. Cloud computing structures have many components as taking after:

- Highly abstracted resources
- Instantaneous provisioning
- Near instant scalability and edibility
- Shared resources (hardware, database, memory, etc.)
- service on demand
- Programmatic management (e.g., through WS API)

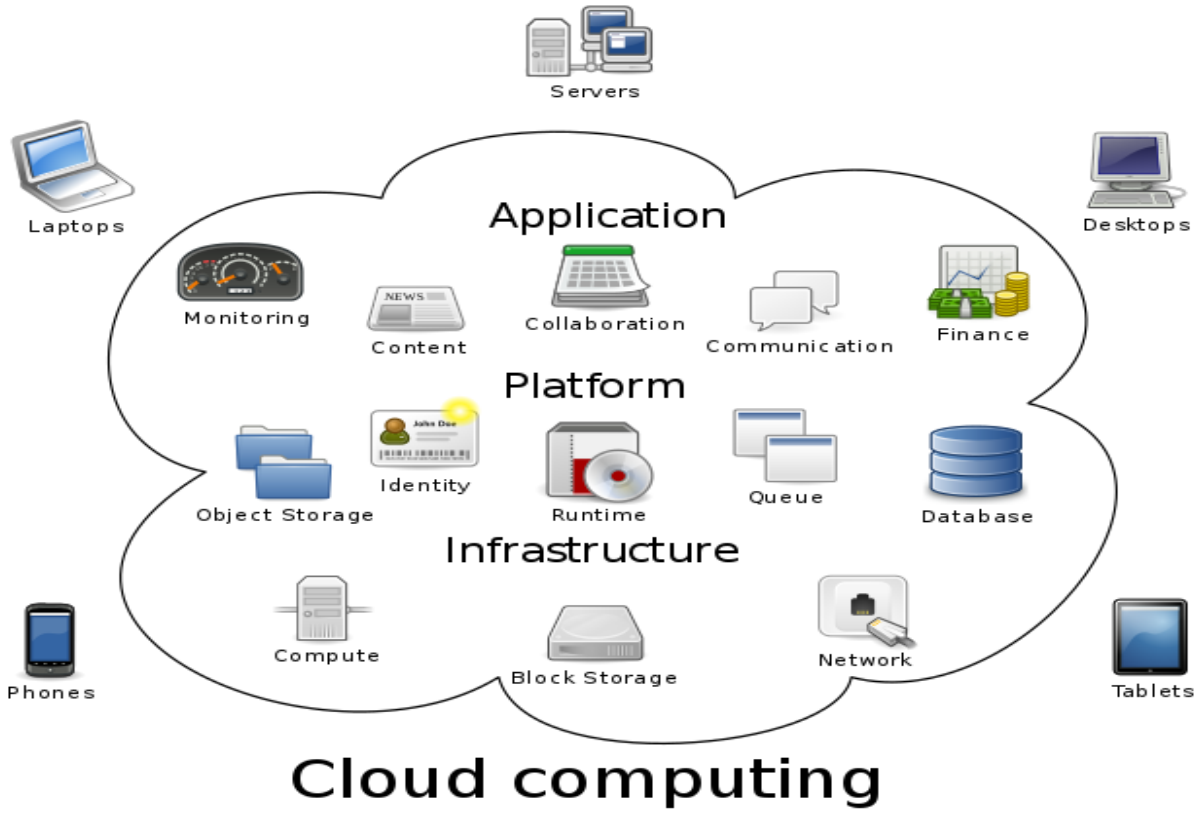

Figure 3.5: Cloud computing model created by sam Johnston 2009 update 2016

Cloud computing metaphor: for a user, the network elements representing the provide rendered services are invisible, as if obscured by a cloud.

3.8 Private cloud

Private cloud will be cloud infrastructure worked exclusively for a solitary association, regardless of whether oversaw inside or by an outsider, and facilitated either inside or remotely by Mell and Grance, (2011). Undertaking a private cloud extend requires a noteworthy level and level of arrangement to virtualize the business condition, and requires the association to reexamine choices about existing assets. At the point when done right, it can enhance business, yet every progression in the venture raises security issues that must be routed to forestall genuine vulnerabilities. Self-run server farm are by and large capital concentrated. They have a critical physical impression, requiring portions of space, equipment, and ecological controls. These advantages must be invigorated occasionally, bringing about extra capital consumptions. They have pulled in feedback since clients "still need to purchase, construct, and oversee them" and in

this manner don't profit by less involved administration, basically lacking the monetary model that makes distributed computing such a charming idea". (Haff, Gordon, 2010).

3.9 Public cloud

A cloud is known as a "public cloud" when the administrations are rendered over a system that is open for open utilize. Open cloud administrations might be free Margaret, (2014). Technically there might be practically no contrast amongst open and private cloud design, nonetheless, security thought might be significantly unique for administrations (applications, stockpiling, and different assets) that are made accessible by a specialist co-op for an open gathering of people and when correspondence is affected over a non-confided in system. For the most part, open cloud specialist organizations like Amazon Web Services (AWS), Microsoft and Google claim and work the foundation at their server farm and get to is for the most part through the Internet. AWS and Microsoft likewise offer direct associate administrations called "AWS Direct Connect" and "Purplish blue ExpressRoute" individually, such associations oblige clients to buy or rent a private association with a peering point offered by the cloud supplier.

3.10 Hybrid cloud

Hybrid cloud is structures of at least two mists (private, community or public) that stay unique elements however are bound together, offering the advantages of numerous sending models. Half breed cloud can likewise mean the capacity to interface collocation, oversaw or potentially devoted administrations with cloud assets. Bittman, (2015), characterizes a hybrid cloud benefit as a distributed computing administration that is made out of some blend of private, open and group cloud administrations, from various specialist co-ops. A half and half cloud benefit crosses seclusion and supplier limits so it can't be essentially placed in one classification of private, public, or community cloud benefit. It enables one to amplify either the limit or the capacity of a cloud benefit, by conglomeration, reconciliation or customization with another cloud benefit, (Kaewkasi, 2015).

Fluctuated utilize cases for hybrid cloud arrangement exist. For instance, an organization may store touchy customer information in house on a private cloud application, however interconnect that application to a business knowledge application given on an open cloud as a product benefit. This case of hybrid cloud expands the capacities of the undertaking to convey a particular

business benefit through the expansion of remotely accessible public cloud administrations. Hybrid cloud appropriation relies on upon various variables, for example, information security and consistence necessities, level of control required over information, and the applications an association employments. (Kaewkasi, 2015).

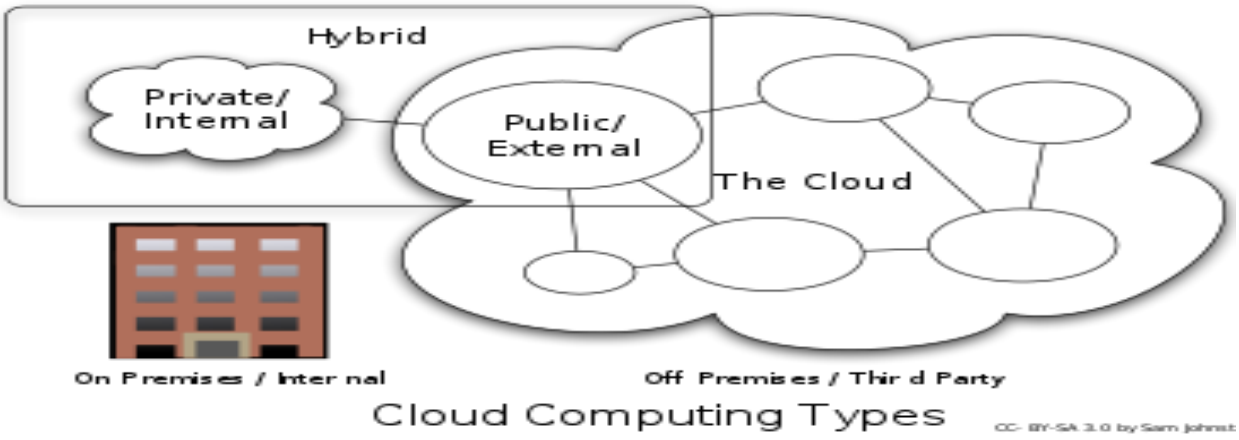

Figure 3.6: Cloud Computing Type Source http://cloudlighthouse.be

Another case of hybrid cloud is one where IT organizations utilize public cloud computing assets to meet transitory limit needs that can't be met by the private cloud. (Desire, 2015).This ability empowers hybrid cloud to utilize cloud blasting for scaling crosswise over mists. Cloud blasting is an application organization demonstrate in which an application keeps running in a private cloud or server farm and "blasts" to an public cloud when the interest for figuring limit increments. An essential favorable position of cloud blasting and a hybrid cloud model is that an organization pays for additional compute assets just when they are required. Cloud blasting empowers data center to make an in-house IT framework that backings normal workloads, and utilize cloud assets from public or private clouds, amid spikes in handling requests. The particular model of hybrid cloud, which is worked on heterogeneous equipment, is called "Cross-stage Hybrid Cloud". A cross-stage hybrid cloud is typically fueled by various CPU structures, for instance, x86-64 and ARM, underneath. Clients can straightforwardly convey and scale applications without learning of the cloud's equipment differing qualities (Kaewkasi, 2015). This sort of cloud rises up out of the raise of ARM-construct framework in light of chip for server-class processing.

3.11 Community Cloud

A community cloud in computing is a collective exertion in which framework is shared between a few associations from a particular group with basic concerns (security, consistence, ward, and so forth.), regardless of whether oversaw inside or by an outsider and facilitated inside or remotely. This is controlled and utilized by a gathering of organizations that have shared intrigue. The expenses are spread over less clients than an open cloud (yet more than a private cloud), so just a portion of the cost reserve funds capability of cloud computing are acknowledged (Marinos, 2009)

Figure 3.7: Community cloud computing source: http://cloudlighthouse.be

3.12 Distributed Cloud

A cloud computing stage can be gathered from a circulated set of machines in various areas, associated with a solitary system or center administration. It is conceivable to recognize two sorts of disseminated mists: open asset processing and volunteer cloud Vincenzo D. Cunsolo, Salvatore Distefano.

Public-asset processing, this sort of dispersed cloud comes about because of a sweeping meaning of distributed computing, since they are more similar to appropriated figuring than distributed computing. In any case, it is viewed as a sub-class of distributed computing, and a few illustrations incorporate conveyed registering stages, for example, BOINC and collapsing home.

Volunteer cloud, Volunteer distributed computing is portrayed as the convergence of open asset registering and distributed computing, where a distributed computing framework is fabricated

utilizing volunteered assets. Many difficulties emerge from this kind of foundation, in view of the instability of the assets used to construct it and the dynamic condition it works in. It can likewise be called shared mists, or specially appointed mists. A fascinating exertion in such heading is Cloud Home; it means to execute a distributed computing foundation utilizing volunteered assets giving a plan of action to boost commitments through money related compensation.

3.13 Intercloud

The Inter-cloud is an interconnected worldwide "billow of mists and an expansion of the Internet "system of systems" on which it is based. The attention is on direct interoperability between open cloud specialist organizations, more so than amongst suppliers and purchasers (just like the case for mixture and multi-cloud (Canada 2007, Head in the mists? Welcome to the future Toronto)

3.14 Multicloud

Multicloud is the utilization of various distributed computing administrations in a solitary heterogeneous design to decrease dependence on single sellers, increment adaptability through decision, alleviate against calamities, and so forth. It contrasts from half breed cloud in that it alludes to various cloud administrations, as opposed to different organization modes (open, private, and heritage).

3.15 Cloud Computing Service Models

Service models CC can be accessed through an set of services models. These services are designed to exhibit certain characteristics and to satisfy the organizational requirements. From this, a best-suited service can be selected and customized for a organization’s use. Some of the common distinctions in cloud computing services are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure as a Service (IaaS), Hardware-as-a-Service (HaaS) and Data storage as a Service (DaaS) Service model details are as follows:

3.15.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) is a form of cloud computing that provides virtualized computing resources over the Internet. IaaS is one of three main categories of cloud computing services, alongside Software as a Service (SaaS) and Platform as a Service (PaaS). In an IaaS

model, a third-party provider hosts hardware, software, servers, storage and other infrastructure components on behalf of its users. IaaS providers also host users' applications and handle tasks including system maintenance, backup and resiliency planning, Rose (2017). IaaS platforms offer highly scalable resources that can be adjusted on-demand. This makes IaaS well-suited for workloads that are temporary, experimental or change unexpectedly. Other characteristics of IaaS environments include the automation of administrative tasks, dynamic scaling, desktop virtualization and policy-based services (Rose, 2017).

IaaS customers pay on a per-use basis, typically by the hour, week or month. Some providers also charge customers based on the amount of virtual machine space they use. This pay-as-you-go model eliminates the capital expense of deploying in-house hardware and software. However, users should monitor their IaaS environments closely to avoid being charged for unauthorized services Margaret Rose (2017 By utilizing this kind of service, user has control over operating framework, storage, deployed applications and potential, limited control over designated framework assets. Examples of IaaSclouds are Eucalyptus (The Eucalyptus Open source Cloud computing System), EC2 Amazon, Rack space, and Nimbus cloud (Rose, 2017).

3. 15.2 Platform as a Service (PaaS)

Platform as a service (PaaS) or application Platform as a service (aPaaS) is a classification of distributed computing administrations that gives a stage enabling clients to create, run, and oversee applications without the multifaceted nature of building and keeping up the framework normally connected with creating and propelling an application ohn (Wiley and Sons, 2012). PaaS can be conveyed in two routes: as an open cloud benefit from a supplier, where the customer controls programming arrangement with negligible design choices, and the supplier gives the systems, servers, stockpiling, OS, "middleware" (e.g. Java runtime, NET runtime, joining, and so on.), (Hoboken, NJ: John Wiley and Sons, 2012). Database and different administrations to have the customer's application, or as a private administration, (software orapparatus) inside the firewall or as programming conveyed on an open framework, as a service (Gartner IT Glossary, 2015).

PaaS gives a situation to designers and organizations to make have and send applications, sparing engineers from the complexities of the framework side (setting up, arranging and

overseeing components, for example, servers and databases). PaaS can enhance the speed of building up an application, and enable the shopper to concentrate on the application itself. With PaaS, the shopper oversees applications and information, while the supplier (out in the open PaaS) or IT office (in private PaaS) oversees runtime, middleware, working framework, virtualization, servers, stockpiling and systems administration. Advancement devices given by the seller are altered by the requirements of the client. The client can keep up the product, or have the seller keep up (Brandon Butler, 2013).

3.15.2.1 Advantages and Disadvantage of Paas,

The upsides of PaaS are fundamentally that it takes into account larger amount programming with significantly decreased multifaceted nature; the general advancement of the application can be more compelling, as it has worked in foundation; and support and upgrade of the application is less demanding (Cloud Computing Stack, Rackspace 2013). It can likewise be helpful in circumstances where various designers are dealing with a solitary venture including parties who are not found nearby.

One inconvenience of PaaS offerings is that engineers will be unable to utilize a full scope of ordinary devices (e.g. social databases, with unlimited joins). Another conceivable burden is being secured to a specific stage. In any case, most PaaSes are moderately secure free. (William Y. Chang, Hosame Abu-Amara, Jessica Feng Sanford 2010)

3.15.3 Software as a Service (SaaS)

Keeping up software applications licenses can be tedious and frequently "fly up" as an unbudgeted cost. On location licenses likewise require a pledge to licenses that may not be required in months to come as association's streamline business prepare prompting fluctuating headcount. Programming as Service Software organizations are currently giving the chance to expend licenses in view of Software as a Service. In the software as a service (SaaS) demonstrate, clients access application programming and databases. Cloud suppliers deal with the framework and stages that run the applications. SaaS is now and then alluded to as "on-request programming" and is generally estimated on a compensation for every utilization premise or utilizing a membership expense (Ziff. D, 2014). In the SaaS demonstrate, cloud suppliers introduce and work application programming in the cloud and cloud clients get to the

product from cloud customers. Cloud clients don't deal with the cloud framework and stage where the application runs. This dispenses with the need to introduce and run the application on the cloud client's own particular PCs, which rearranges upkeep and support. Cloud applications vary from different applications in their versatility which can be accomplished by cloning undertakings onto various virtual machines at run-time to take care of changing work demand. Stack balancers disperse the work over the arrangement of virtual machines. This procedure is straightforward to the cloud client, who sees just a solitary get to point. To oblige countless clients, cloud applications can be multitenant, implying that any machine may serve more than one cloud-client organization.

The estimating model for SaaS applications is regularly a month to month or yearly level charge per client (Intrinsic Technology, 2012) so costs wind up plainly versatile and movable if clients are included or expelled anytime. Advocates assert that SaaS gives a business the possibility to diminish IT operational expenses by outsourcing equipment and programming upkeep and support to the cloud supplier. This empowers the business to reallocate IT operations costs far from equipment/programming spending and from work force costs, towards meeting different objectives. What's more, with applications facilitated midway, updates can be discharged without the requirement for clients to put in new programming. One downside of SaaS accompanies putting away the clients' information on the cloud supplier's server. Subsequently, there could be unapproved access to the information. Therefore, clients are progressively receiving clever outsider key-administration frameworks to help secure their information.

3.15.4 Hardware as a Service (HaaS):

Hardware as a Service (HaaS) is a package arrangement display for equipment that is characterized contrastingly in overseen services and lattice processing settings. In oversaw services, (Margaret, 2016), HaaS is like permitting in framework registering, HaaS is a compensation as-you-go demonstrates. Buying an equipment or a whole datacenter with a compensation as-you-utilize scheme which can scale all over according to client necessities can be named as Hardware as a Service (HaaS). Cases for HaaSclouds are Amazon EC2, IBM's Blue Cloud Project, Nimbus, Eucalyptus, and Anomalism.

3.15.5 Identity as a Service (IDaaS)

Identity alludes to set of ascribes related with something to make it recongizable. All articles may have same characteristics, yet their personalities can't be the same. A unique identity character is doled out through remarkable recognizable proof characteristic. Hardware as a service is part of a bigger layered security technique. Its essential duty is regulatory as far as making client qualifications and allotting them to specific containers of consent. This provisioning depends on the part of client serves inside an association. Offices or divisions see one bit, accomplices see another, clients another each lone is allowed to get to exactly what they require (Cloud Tech News 2013).

There are a few personality benefits that are conveyed to approve administrations, for example, approving sites, exchanges, exchange members, customer, and so forth. Way of life as-a-Service may incorporate the accompanying:

- Directory services
- Federated services
- Registration service
- Authentication services
- Risk and event checking
- Single sign-on administrations
- Identity and profile administration

Workers in an organization require to login to framework to perform different undertakings. These frameworks might be founded on nearby server or cloud based. Taking after are the issues that a worker may confront: Recollecting diverse username and secret key blends for getting to different servers. On the off risk that a representative leaves the organization, it is required to guarantee that each record of that client is debilitated. This builds workload on IT staff.

IDaaS offers administration of personality data as a computerized substance. This personality can be utilized amid electronic exchanges. Identification identify a set of ascribes related with something to make it conspicuous. All items may have same properties; however their characters can't be the same. A special character is doled out through one of a kind distinguishing proof property.

3.15.6 Anything as a Service (XaaS):

XaaS is an aggregate term said to remain for various things including "X as a service," "anything as a service" or "everything as a service." The acronym alludes to an expanding number of services that are conveyed over the Internet as opposed to give locally or on location. XaaS is the substance of distributed computing. This is more broad type of speaking to sending of an administration. These services could be of any sort and "X" in XaaS can be substituted by programming, equipment, infrastructure, information, business, IT, Security, observing, and so forth. Nowadays new service models are being produced. Illustrations are: IT as an administration, Cloud as a Service (CaaS), Management as a Service (MaaS), and so on, is some different administrations that are recognized in writing (Margaret, 2016).

3.15.7 Privacy and Anonymization as a Services:

As a Service (PAAS): This service is proposed as a showing model to give information security and insurance in a specific organization. It likewise proposes a work process situated way to deal with oversee information in cloud.

3. 15.8 Data storage as a Service (DaaS):

This service allows user to pay for data storage he/she is using. With this service there is a separate cloud formed which provides storage as a service. Examples of such kinds of clients are Amazon S3, Google Bigtable, ApacheHbase.

3.15.9 Security as a Service (SaaS):

This service allows users to create their own security policies and risk frameworks. In this kind of service, cloud users must identify, assess, and measure and prioritize system risks.

3.16 Virtualization in Data Centers

Server virtualization has turned out to be main-stream in Data Center since it gives a simple component to neatly parcel physical assets, enabling different applications to continue running in segregation on a cloud server. Virtualization assists with server combination and gives adaptable asset administration instruments, although it can present new difficulties.

Figuring out where to run applications in a common domain remains a test, and virtualization adds new troubles because of the variable virtualization overheads seen by various applications and stages. Our work investigates another element to consider while setting VMs, the potential for memory sharing, and gathers models that describe VM overheads.

Some business frameworks now exist for mechanizing the administration of VM assets and an assortment of research projects have proposed plans for administration of handling and memory assets. This work was a portion of the first to join mechanized administration of VM assets with dynamic relocation to adjust stack inside business data centers.

Unwavering quality is an essential component for data center applications, and virtualization has existed utilized to offer expanded strength even with crash disappointments. This work extends these thoughts to give disaster recovery benefits crosswise over data centers, enabling applications to bomb over starting with one then onto the next without any information misfortune. This audit proposes another replication approach in view of the thoughts of outer synchrony, which utilizes theoretical execution to consolidate the best parts of synchronous and off beat methodologies.

3.17 Summary

In this chapter the basic knowledge of cloud computing, cloud migrating, assessment and its development status are firstly introduced. The definitions of deployment models as well as the classification of migration types are applied as foundation concerns of this work. Then we refer to the concept of decision support system by sharing several models and framework for cloud adoption, which is used to simplify the risk identification for the users in this work. At last, a general understanding of risk management according to ISO 31000 is given with its framework and process, which over a hint of how to identify and assess the risks in cloud migration.

CHAPTER FOUR
METHODOLOGY

In this chapter, we define the Service Blueprints that model interactions and roles of Information Risk Management (IRM), Infrastructure and Operations (I&O), and the App Owners during Development (planning) and Deployment (DR) phases, providing insight to the internal customer/provider dynamics within the Enterprise. This documentation helps model roles and key interactions for effective DR Triage.

We also introduce the concept of App Suites and discuss in detail the AS-IS analysis, Challenges identified and the key underlying Principles that guide the proposed solution. Risk analysis methodology is structure as four distinct phases: Risk analysis of resources, controls, threats, and vulnerabilities. Management decisions to implement security counter measures, and accept residual risk and periodic review of the risk management program. This document addresses the first phase; which provides the foundation for the remaining three phases.

4.1 Service Blueprint – Development

The Development Service Blueprint models interactions and roles of IRM, I&O and the Business Solution Areas (BSAs) during Development phase of this project. It is IRM driven, and I&O is the customer.

Recovery Requirements (objectives, data currency, redundancy, load balancing etc.) come from the BSAs and IRM understands the requirements, gathers AS-IS information (infrastructure, data, services, roles, etc.) and may further engage in discussions regarding compliance objectives. IRM then reaches out to I&O, which would identify App and Tech interdependencies, and determine App Suite RTAs. IRM would then, using the Recovery Sequence Algorithm propose an optimized recovery sequence, report on gaps in meeting business recovery objectives and associated costs, and provide DR feedback to the BSAs attempting to converge RTAs and RTOs via the Continuous Improvement program.

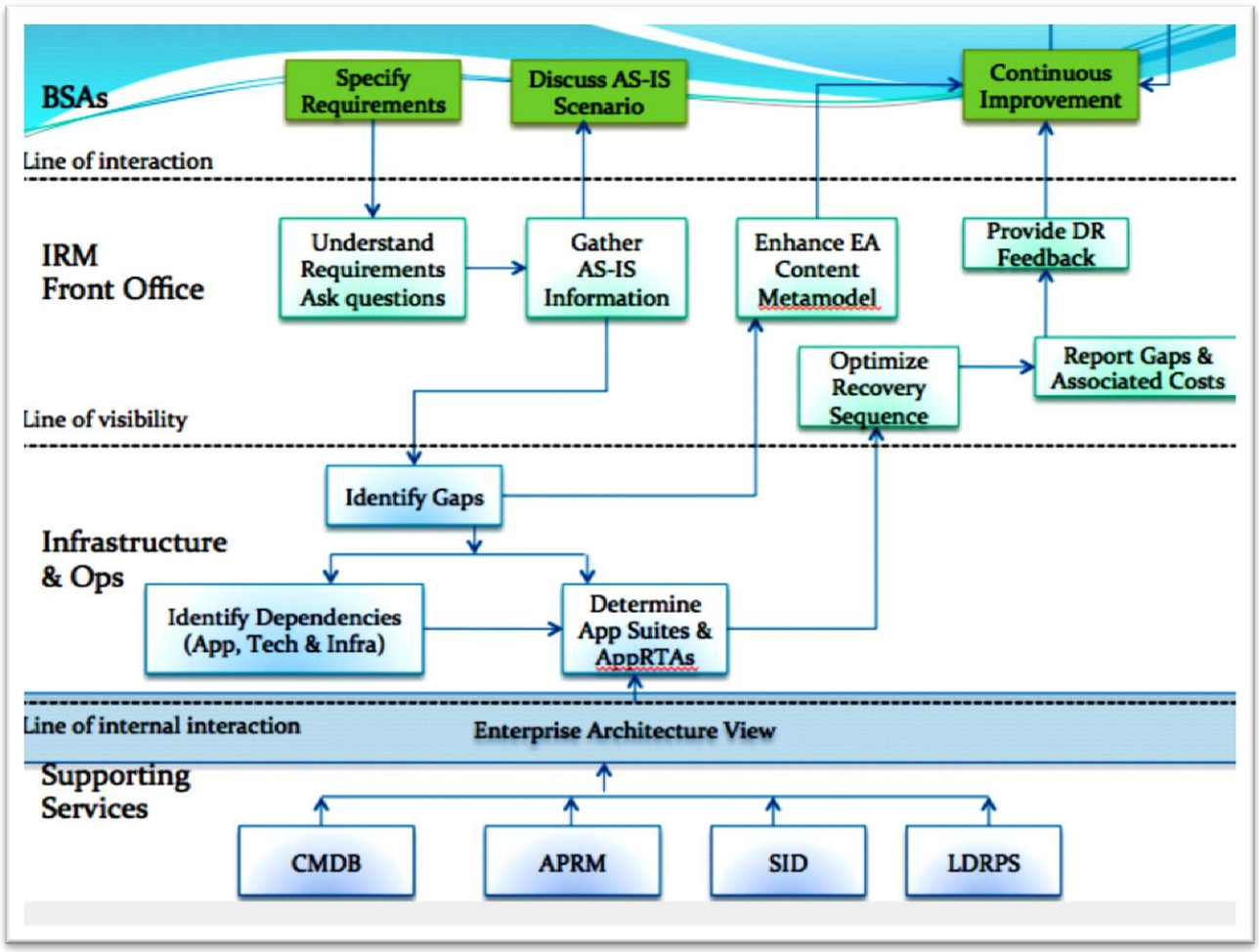

Figure 4.1: Development Service Blueprint

4.2 Service Blueprint – Deployment

The Deployment Service Blueprint models interactions and roles of IRM, I&O and the Enterprise during Deployment (At Time of Disaster!) phase of this project. It is I&O driven, and the Enterprise is the customer.

The Enterprise Command Center would declare the disaster and the Enterprise would then be in a state known as Mission Critical. Only a fraction of the employees, typically I&O and Business Continuity (IRM) would be engaged and would work **c**losely with App teams to get the Infrastructure up, Data verification and Sync processes initiated.

The App Teams would be the ones requesting a move to the Recovery Datacenter and IRM would be involved in DR Triage and engaging I&O, which would then drive this process. I&O

would get its information from various underlying databases via the ubiquitous EA View, to identify App and Tech interdependencies and determine App Suites to be recovered. IRM would then present a dashboard visualization of the optimized recovery sequence, minimizing cost of downtime for the Enterprise, whilst I&O would bring up the Infrastructure. It would then be back to the App teams for Data Verification and Sync, ensuring Business Continuity after the disaster.

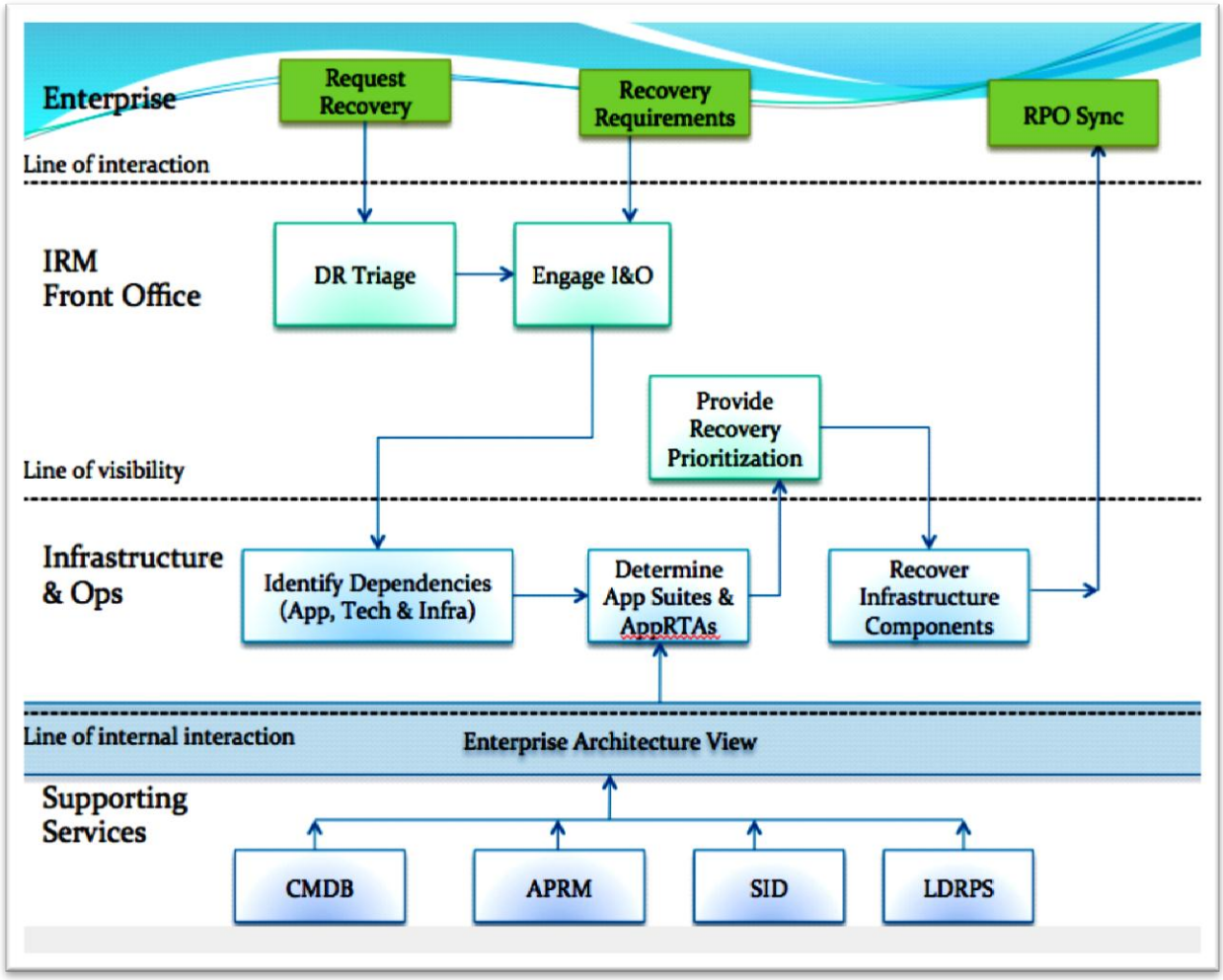

Figure 4.2: Deployment Service Blueprint

4.2.1 Concept of App Suites

An App Suite consists of an App along with its sub-network components (data and dependencies). The key significance in defining this notation is to provide visibility of dependencies across Business Processes, and to have fine-grained control over prioritizing each App within a Business Process.

An App Suite once recovered, impacts Apps from other Business Processes as their remaining Time to recover now goes down as App and Tech Dependencies across Business Processes get recovered. The App Suite abstraction, allows us to dynamically update recovery priority based on dependencies that have been recovered.

A Business Process may contain non-essential Apps that need not be recovered to restore critical functionality and hence the need for prioritizing recovery of subset of Apps supporting that Business Process. This can be visualized as a Depth-first-search approach where App Suites are recovered, versus a more conventional Breadth-first-search approach of recovering all Apps in a Business Process and then proceeding to dependencies or other less critical Business Processes.

Apps having lower criticality might be indirectly supporting higher criticality Apps, and would hence require additional budgeting for meeting the associated higher thresholds of recovery capability, expected of an App being recovered as part of a highly critical App Suite.

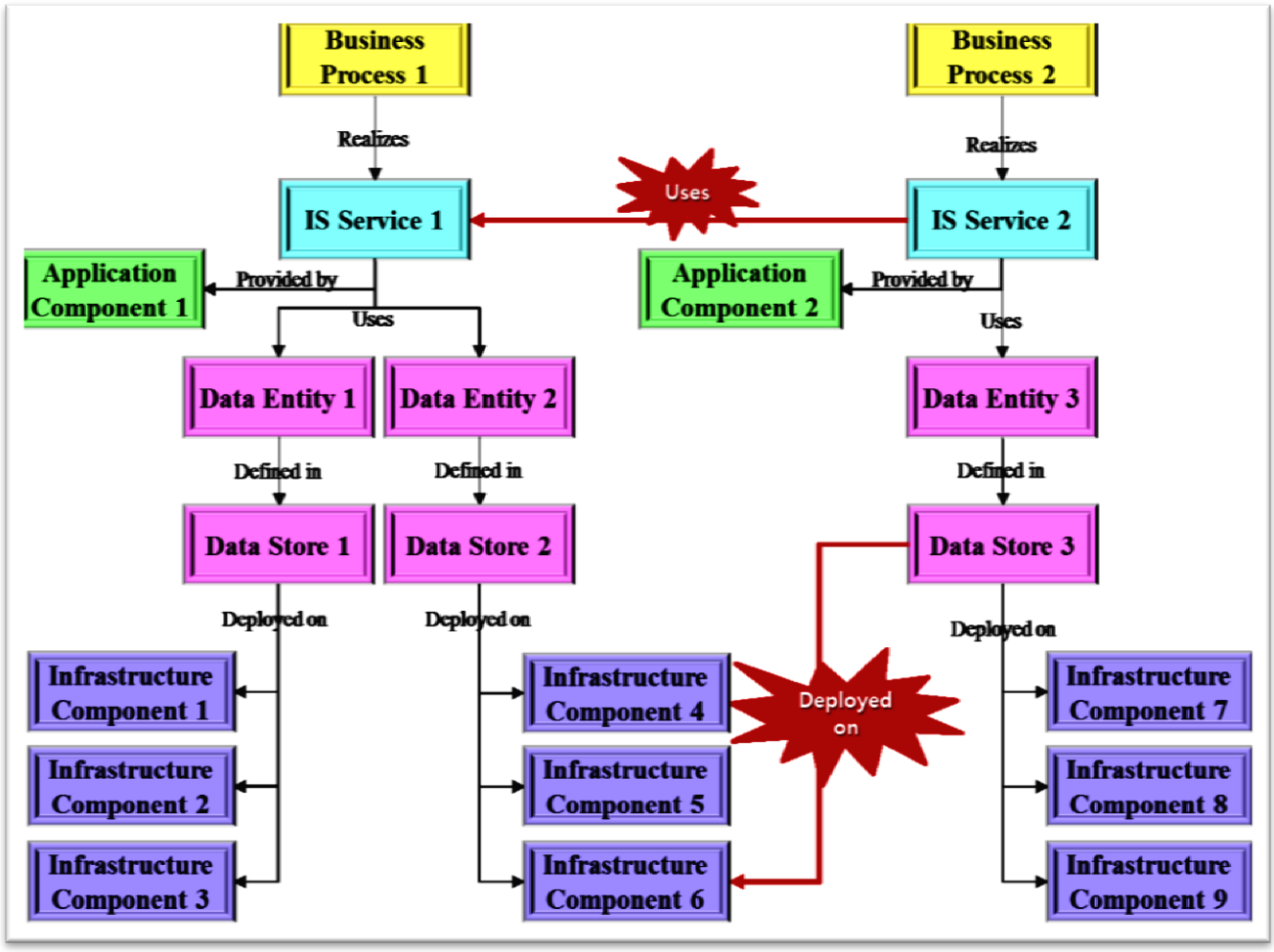

Figure 4.3: AS-IS for a given server

4.2.2 Intermediary Database Example

The example in Figure 10 denotes Business Processes BP1 and BP2, and their associated primary and secondary components. BP1 and BP2 are two Business Processes having Recovery Time Objectives (RTOs) of 8hrs and 16hrs respectively. The RSA algorithm will prioritize BP1 over BP2, recovering Infrastructure Components (ICs) 1-6, followed by ICs 7-9. As IC 6 is a shared component, once it's recovered for BP1, Data Store 3 of BP2 can start its Data Sync processes whilst IC 7-9 are recovered, hence benefiting from shared components being already recovered.

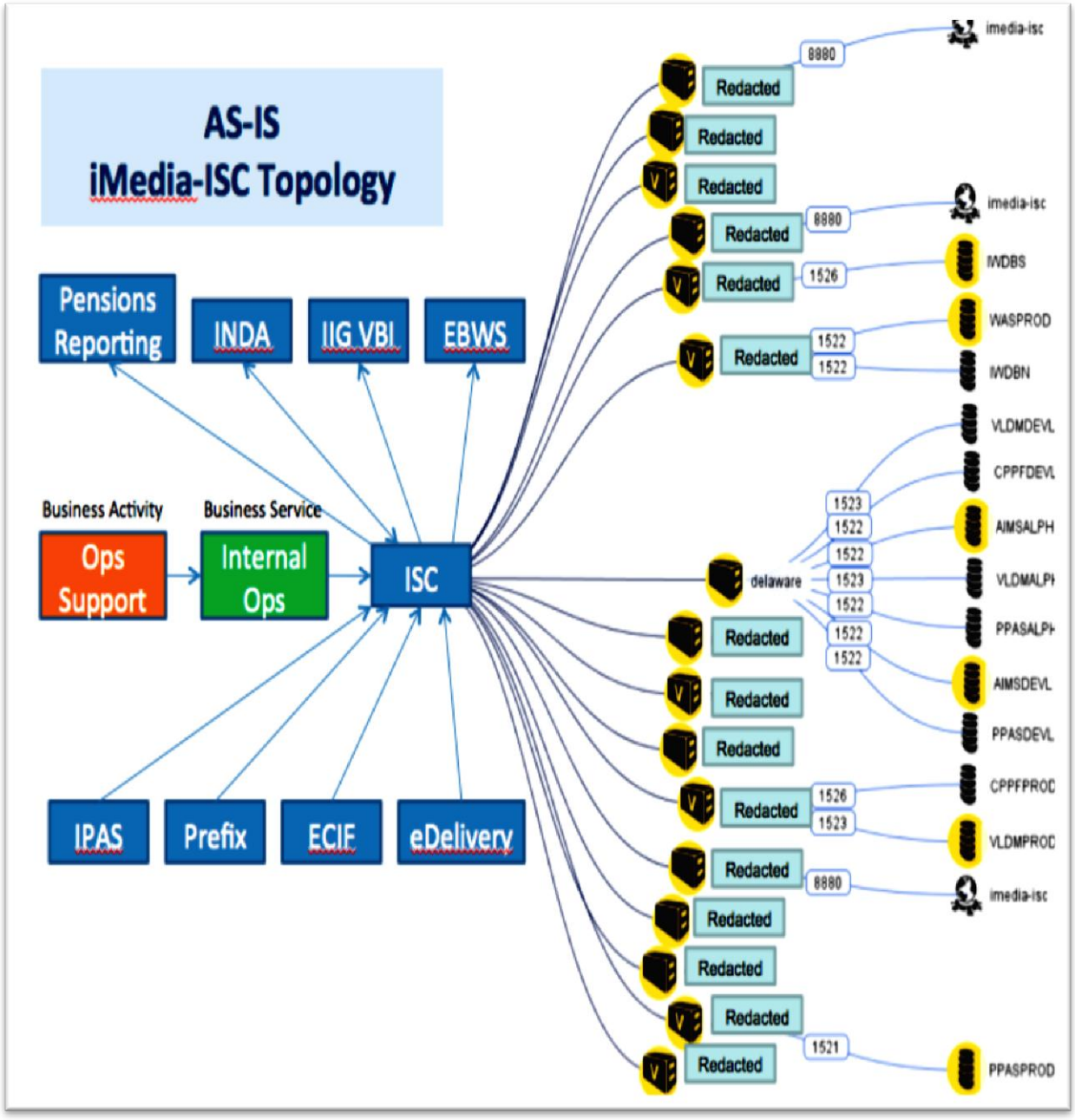

Figure 4.4: AS-IS for a given App

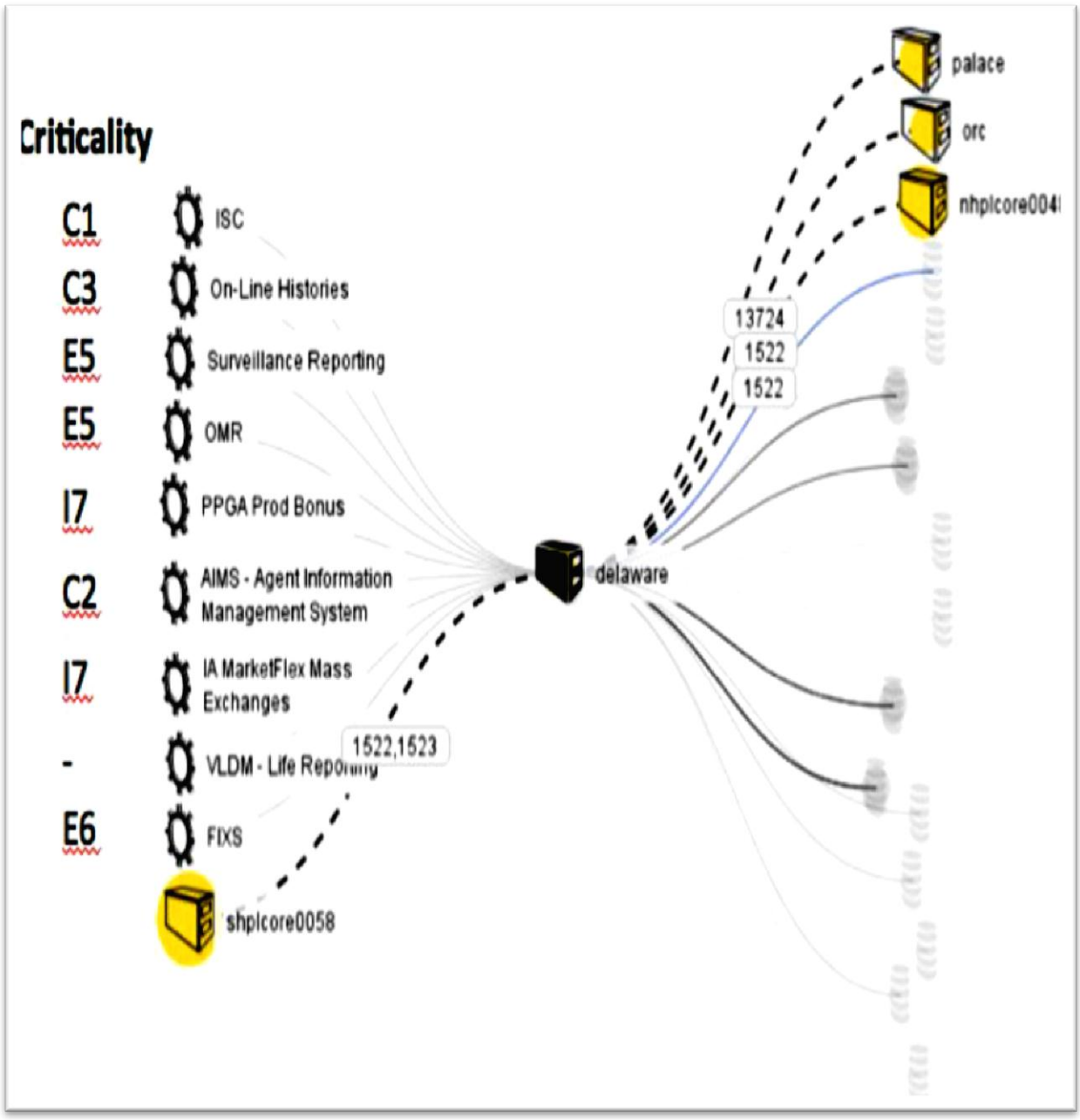

Figure 4.5: AS-IS for a given server

This view (Figures 4.5 and 4.6) is from Athena (the CMDB front-end). It gives a single-level dependency view with respect to Infrastructure and App dependencies. This greatly restricts visibility and capability to do a deep-dive to identify Decision Support Metrics such as RTO/RTA and RPO/RPA that account for nth level of dependencies. It is more of a denotation issue and the inability of the front-end to run reports that fully leverage the power of the CMDB. In addition, the lack of Business Architecture domain metrics in the CMDB does not give the complete picture.

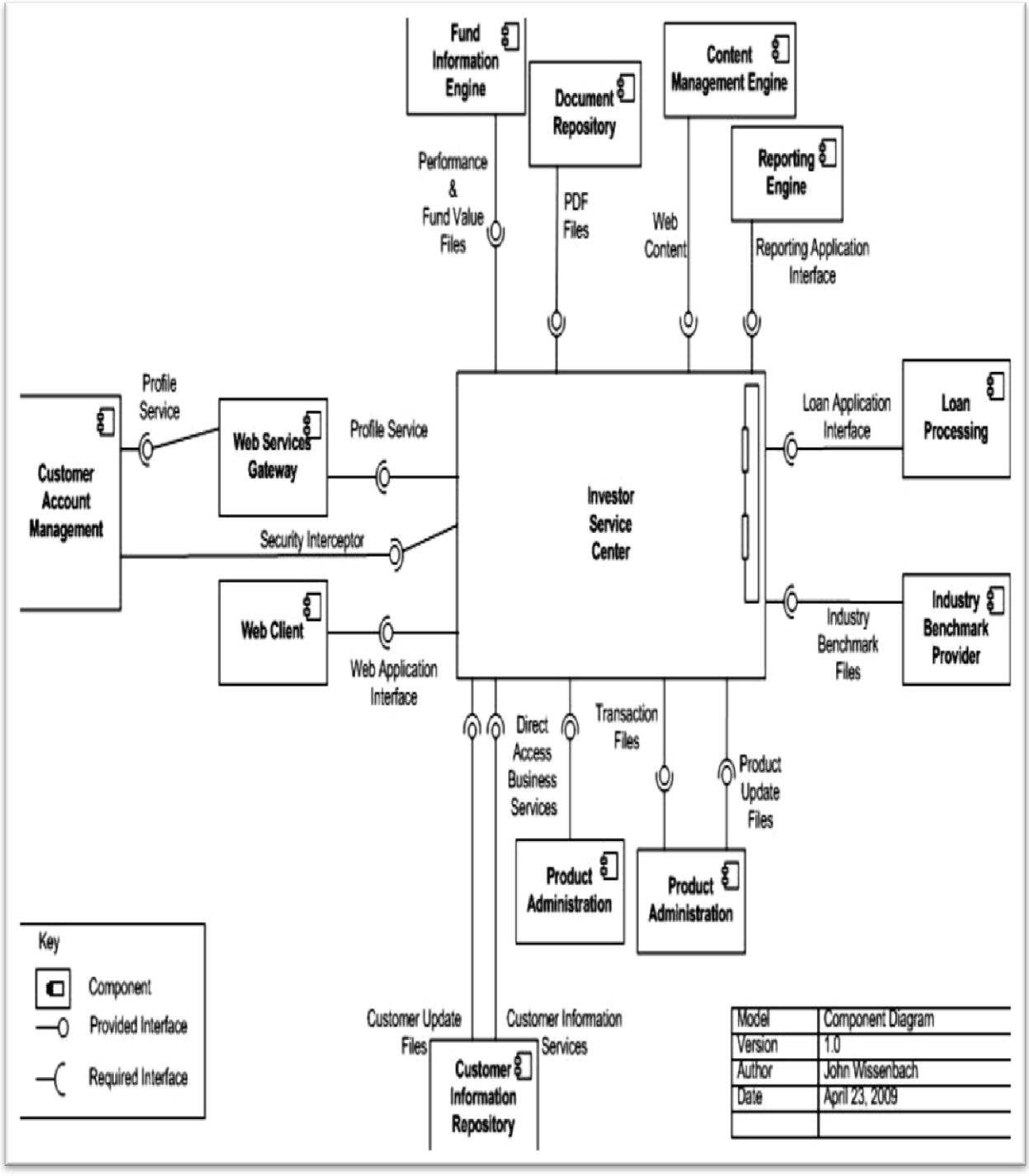

Figure 4.6: AS-IS Component diagram for a given app

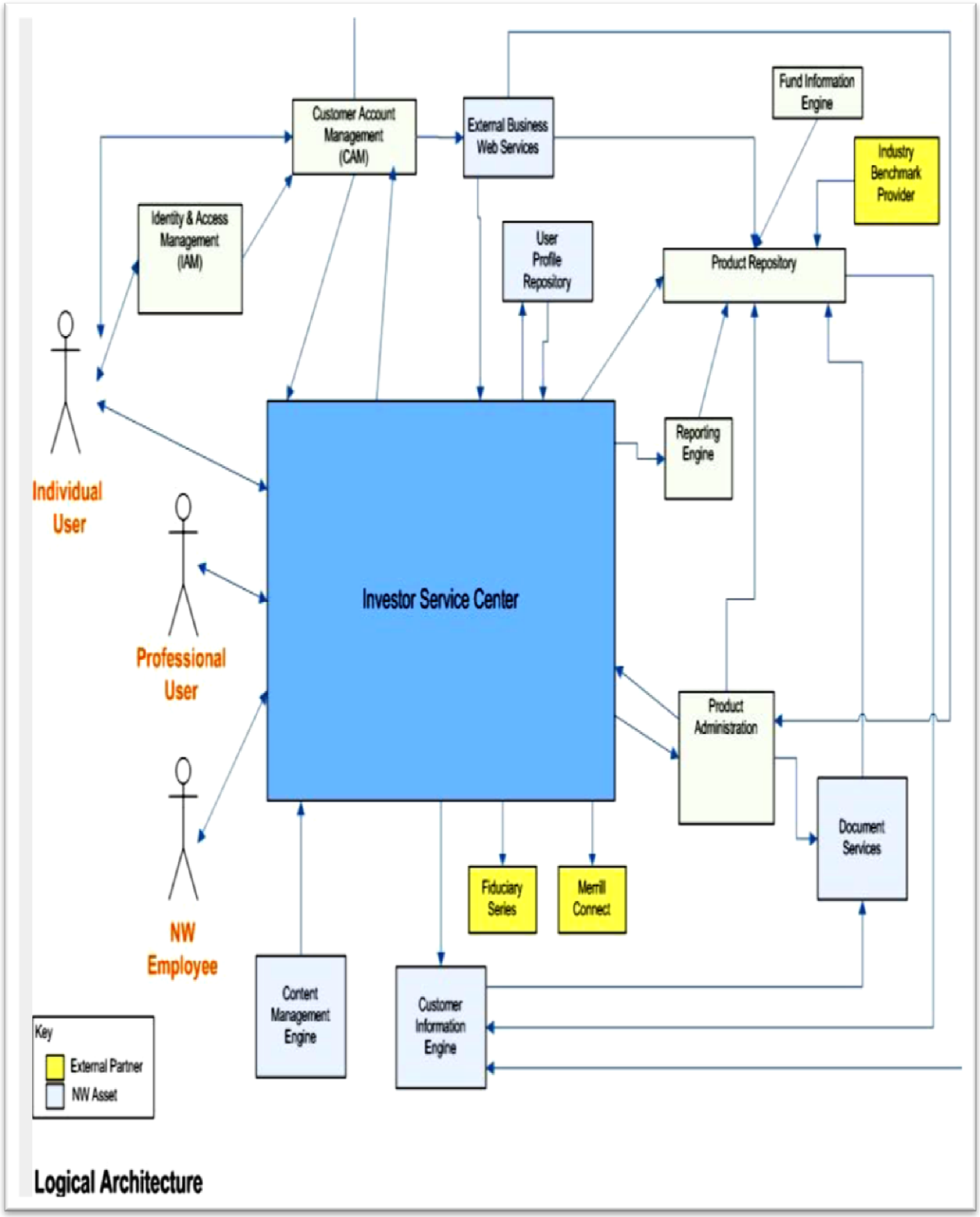

Figure 4.7: AS-IS Logical arch diagram for a given app

Figures 4.5 and 4.6 are the IDEF Component and Logical Architecture views respectively of a sample Critical App we studied as part of the AS-IS analysis. While the specifics are not key to our final end-product, studying the actors, roles and interfaces, helps identify gaps in the current EA Meta-model to help make it truly ubiquitous and relevant, such as in use-cases involving disambiguation in notation for a Virtual Machine vs a standalone Server.

4.3 Challenges that may lead to a sub-optimal solution

Recovery by App Suites (depth-first-search) has a dynamic impact on People, Process and Technology (PPT) that RSA cannot predict or handle optimally with existing metrics. These issues are mainly transitional while adapting from the breadth-first-search recovery paradigm to potentially a more resource intensive RSA approach.

I. This can result in lack of hands on deck (People) i.e. same team might be responsible for recovery of multiple apps having mixed criticality ratings; so an otherwise linear recovery of C1, C2, C3 criticality Apps, may now be unfeasible as all of these Apps may require simultaneous recovery if they're part of the same App Suite.

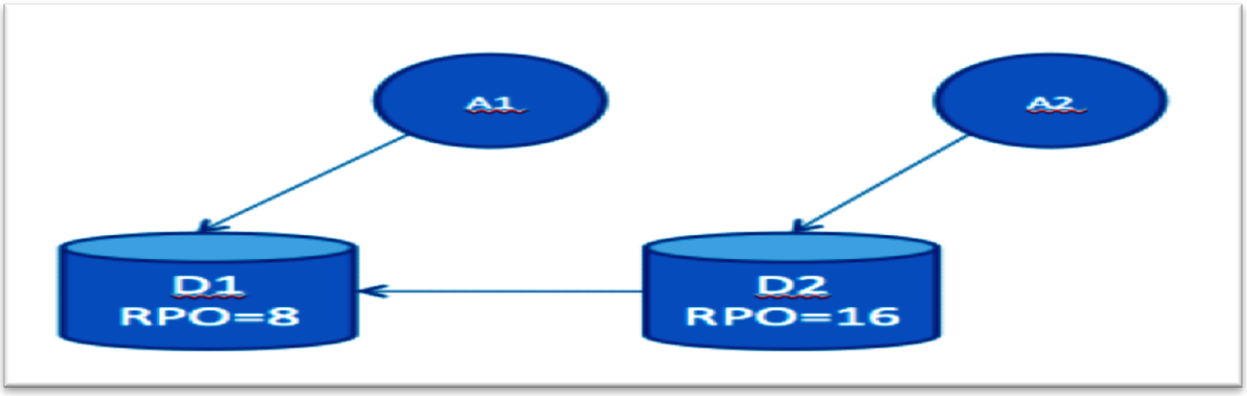

Figure 4.8: Intermediary DB, RPO issue

Dynamic Data Sync/corruption (Process) can result in sub-optimal solution using RSA Recovery.

Intermediary databases (also refer Figure 4.6) to support improved capability assume risk of worst RPO (Data Sync point) in chain of dependencies. It is not common for a new intermediary database. D1 (Figure 4.7) to be created on existing infrastructure for enhanced

capabilities/redundancy, but if it is still dependent on another database D2, having an inferior RPO rating, at Time of Disaster. D1 would need to sync it's data with D2 and would therefore inherit/assume the worst RPO risk in the chain of dependencies as the closest sync point (currency of backup) will be the oldest one for that App Suite therefore involving excessively time consuming Log restores to rebuild databases.

Hardware provisioning (Technology) for low criticality Apps shall be on a timeline of greater than three days, but our proposed solution of recovering App Suites, promotes an App irrespective of its own criticality as long as it supports higher criticality Apps that may require to be "up" within 8hrs. This is again a budgeting issue and convergence of business objectives with current capability, must enable the transition to RSA recovery.

4.4 Principles

Prioritize recovery of Apps by Criticality, which is nothing but the RTO for a given App. An App inherits an attribute from the Business Process it was initially made to support. It is only intuitive to prioritize recovery of Apps having most financial and operational impact from downtime.

Prioritize Apps of given Criticality, by Time Remaining to Recover. For a given set of Apps having the same Criticality rating (i.e. identical dollar loss for identical downtime), it would therefore be intuitive to select the App that can be recovered in the least amount of time. Since dollar loss is associated with downtime, and partial recovery of an App does not mean partial functionality, it is imperative to make sure that Critical Apps are up completely and as quickly as possible.

4.5 Limitations

Currently available data restricts parallelizing recovery at the Tech Component level and cannot be used to optimize capacity and load at individual Infrastructure Components. For example, if we know that Linux Servers (Tech Component) in general, will be up in a finite RTA, it isn't possible with current metrics to dynamically manage capacity and deployment of Apps for a Specific Linux Server (Infrastructure Comp) to foster load balancing in a DR scenario. A Business Process may contain non-essential Apps that need not be recovered to restore critical

functionality. For example, a feedback button on a Claims website need not have prioritized backend database availability. This disambiguation requires knowledge about functionality and business requirements to augment the DR metrics such as RTA to make an informed decision on recovery prioritization.

CHAPTER FIVE
DESIGN & IMPLEMENTATION

This chapter focuses how we can combined both on app of risk assessment and disaster recovery as one app by introducing requirements, presenting the specification and the design, and explaining the implementation of a decision support system for Cloud migration. This migration support system aims to model and incorporate the identified risks and mitigation methods in guiding the user through the different types of migration to the Cloud, with an emphasis on the extensibility of the system. This system is based on RESTful services and implemented in Java language.

5.1 Requirements

Currently Cloud Computing is getting a big popularity in IT solutions, which also pay as you-use service with advantage of efficiency, edibility and scalability. Certainly many risks may also happen within the process of migrating to the cloud. In the Section, we have already introduced some methods for risk identification, such as Stakeholder Impact Analysis by Khajeh-Hosseini (2012), and risk category by Karim Djemame 2006. Besides a risk spreadsheet from Plan for Cloud.com is also explained, which is used to discuss risks from different stakeholder perspectives in an arranged meeting.

Furthermore, we have also described all possible risks with their context of occurrence as well as the likelihood and consequences in a _ne detailed IRM template. However, for the user, who is planning to take advantage of the cloud services, there are no direct ways or such a visualized tool concerning the risks that may be confronted to help making decisions whether it is suitable for the migration and how to avoid or mitigate these risks. In addition, with different cloud deployment models and migration types is the migration of components associated with different types of risks, which lead to decision making even more complicated. Therefore, an easy using and efficient decision support system for risk assessment is on demand (David, 2012).

For our assumption, a comprehensive database of risks with information related is as the basis of this system. This database should contain all the risks that may be confronted in cloud migration and as much descriptions of each risk as possible, which describe the attributes and features of these risks. Then a friendly user interface with full functionalities should be provided in the system, which offers a concrete and direct interaction for the decision makers. In this UI an easy

way of collecting user's information is needed: using choices and making ticks instead of entering texts. After all requirements are collected, the system should search for all the associated risks and present them according to the risk types. All the risks should be listed with information, which are needed for the risk assessment. With this information the user can get a general impression about how many risks would occur, and a concrete understanding about which risks in which aspects he may confront, and how to mitigate the impacts of the risks or totally avoid. This will help the user for the future work in decision-making. Besides, this system should also be platform independent in order to getting a better scalability and extensibility.

5.1.1 Specifications

According to the requirements, all the users' information should be logically collected in the user interface. Choosing the deployment model of Cloud whether an application is being migrated to a public cloud or private, or maybe hybrid, is firstly asked for. In order to get a clear understanding of the deployment models, some helping texts or hints could be offered optional. Then a migration type will be asked for choosing, which we have already discussed in the Section 5.1. For the sake of users some hints about the migration types could be provided with expandable buttons as well because the user may have an unclear understanding about the classification of migration type i.e. if they want to migrate only some components in one layer to the cloud they do not know how to choose the corresponding migration type. Besides, a number of questions will be asked to identify risks more accurately. After all requirements are collected, the system should search for all the associated risks and present them according to different risk types. All the main information about each risk should be listed in order such as risk name, type, context of its occurrence, and the mitigation methods as well. With all these information, the user could have a comprehensive understanding about the property of all possible risks and how to avoid or mitigate their consequence. Based on the major features demanded and the existing methods for decision making that we have already introduced in former section, following details should be considered:

5.1.2 Function

The main function of this system is to collect the user requirements before cloud migration and return all the associated risks that may occur in the process of migration with detailed information. This system offers a comprehensive understanding of the risks confronted and their

corresponding mitigation methods and enables helping the user for decision-making. All the functions would be implemented as RESTful Web Services and the interface as a Web application.

5.1.3 Interaction

The system provides a pleasant, simple, user-friendly interface. The user interface acts as the Frontend of the system and a database as Backend. The interaction is realized between the user and the system where a set of requirements will be given by user and a listing of risks with detailed information as a system result.

5.1.4 Data

A risk database should be created, which contains all kinds of information about risks as well as the relationships between risks and deployment models, between risks and migration types, and between risks and all associated questions. Furthermore, all the questions as well as the hint information for selecting deployment models and migration type should also be involved in the database.

5.1.5 System

The system should be designed as program-language-independent as well as platform-independent for a better extensibility and scalability. In addition, all the services can be put in a WAR _le and able to run in other environments.

5.1.6 System Overview

Figure 5.1 gives an overview of the conceptual architecture of the proposed migration decision support system, which is divided in to 2 parts: a user interface acts as Frontend and a risk database as Backend. Interaction will be implemented between UI and database by using RESFful Service. Entering user requirements includes 3 steps: first, once a deployment model for the migrating has been chosen, a series of corresponding risks will be identified. Second step, choosing the migration type will continue to narrow the search field. At last, a list of questions will be asked to ensure the specific risks, especially in some non-technical aspects. After all the requirements are collected, a comparison between user's requirements and risks in database will

be achieved by RESTful service. And the result of RESTful service, which is seen as the result of searching, will be sent back to the user on the UI.

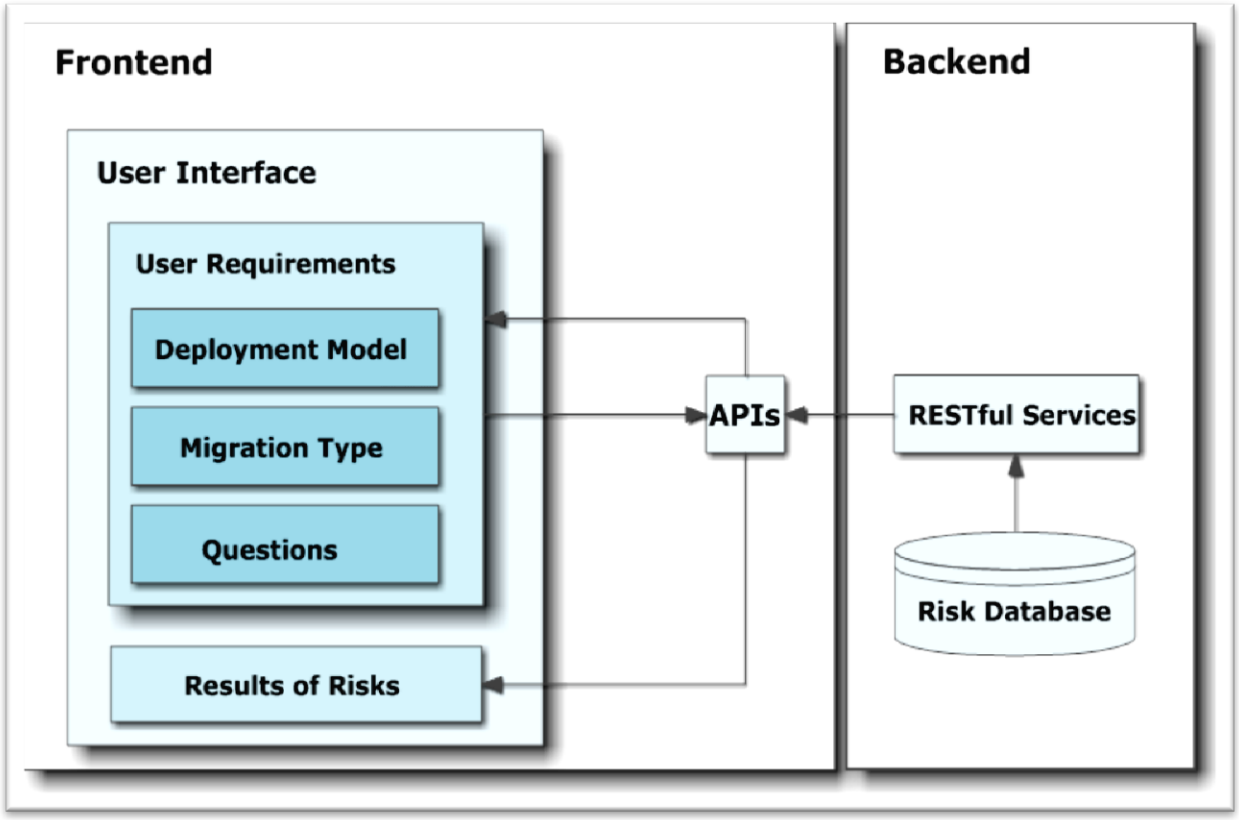

Figure 5.1: Architecture of system

5.1.7 Database

A risk database is the critical part of this system. In each step of decision support process, this database is addressed for offering data and information. Therefore, this database should contain all the risk concerns as well as the relationships between entities. According to the requirement analysis, an Entity-Relation diagram is designed to implement the risk database of the system. This ER-diagram consists mainly of 4 Entities with their attributes and relationships among them, which is presented in Figure 5.2.The entity Risk is as the basic element in the ER-diagram, which all the other entities are related to it. There are 4 deployment models and each model can identify many risks which build these two entities a many-to-many relationship. Similar with the Deployment Model, the Migration Type has also a many-to-many relationship with Risk, since each type is corresponding to many risks. The entity Questions is supposed to have a one-to-many relationship with Risk because certain question can identify many question

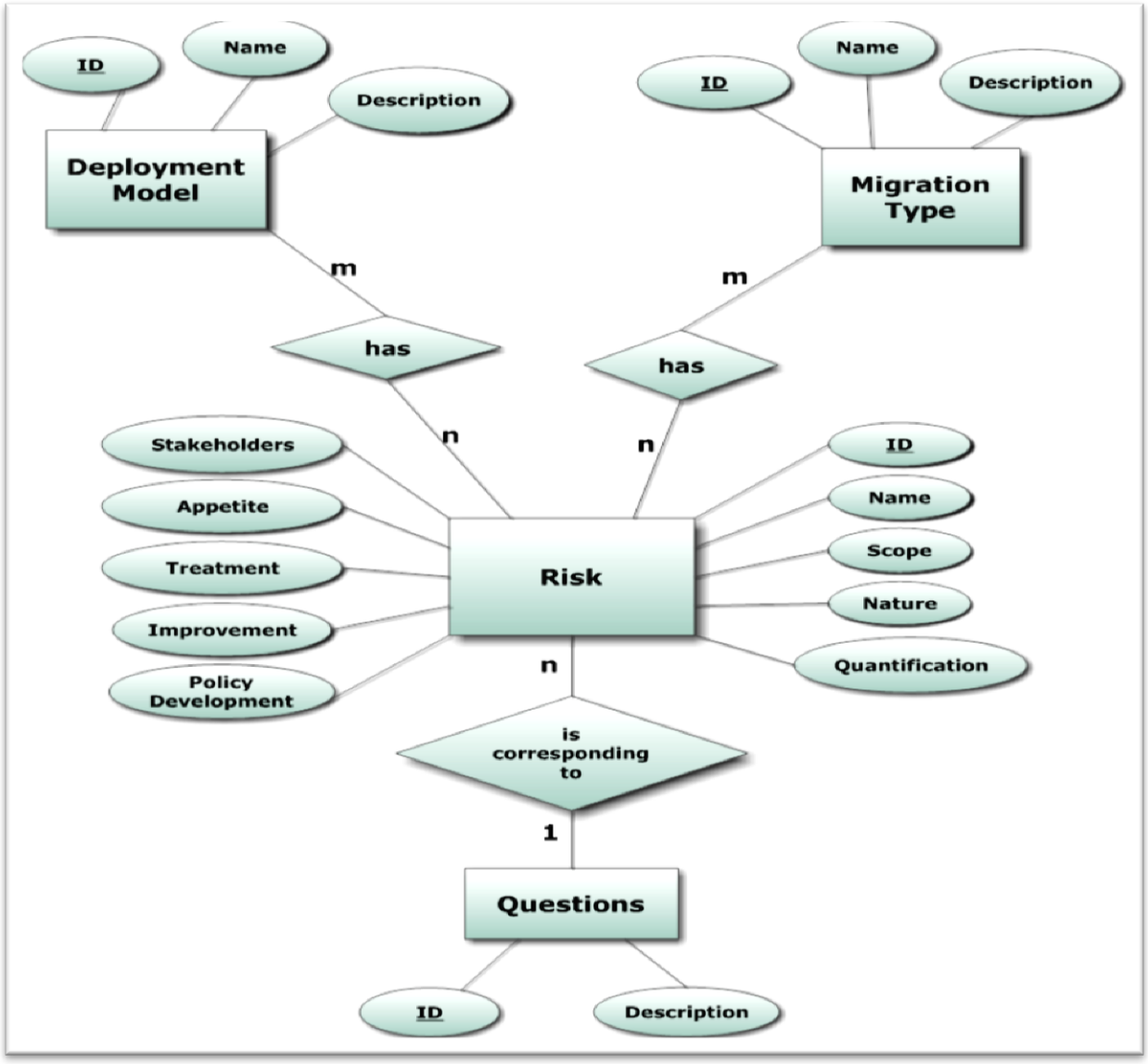

Figure 5.2: ER-Diagram of Risk Database

5.2 User Interface

In this section, the user interfaces of this decision support system are introduced with different scenarios. Balsamiq Mockups is used to set up these UIs, which are presented in following figures. Each UI consists generally of text fields, scroll bars and buttons. Text fields are applied to describe all the requirements as well as the hint information and scroll bar is used to simplify the interface. There are two types of buttons in use, ratio buttons are used to identify the users unique choice while normal button submit the instruction and ask for an execution.

The main page is in Figure 5.3 presented which acts as a dialogue window. It is divided into 2 parts: some system information and a salutatory are located in upper part, and in the lower part, the users' requirements are collected with some hint information shown optional. A scroll bar is on the right side in order to show other information and a main button for submitting the search order is at the bottom.

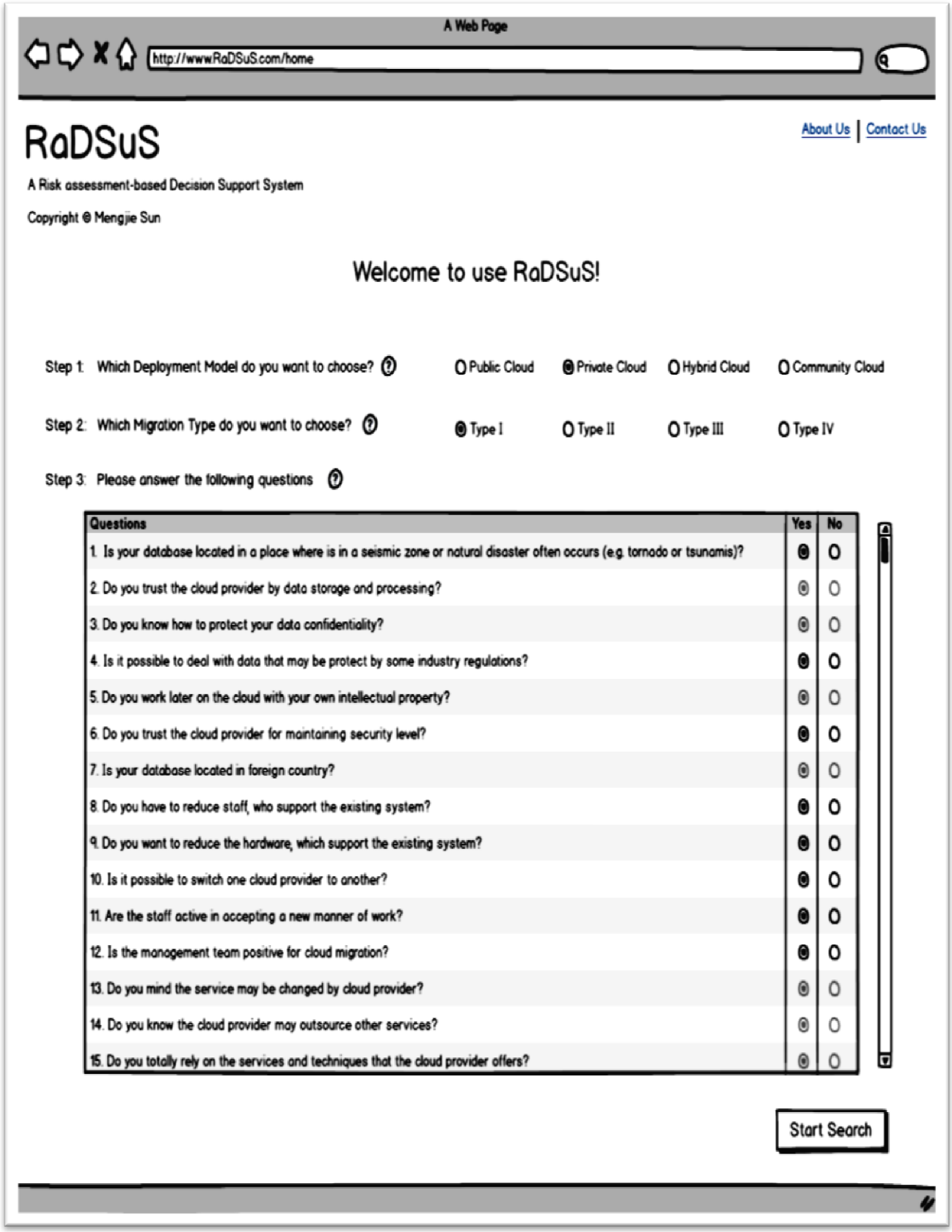

Figure 5.3: Homepage of RaDSuS

As demonstrated in Figure 5.3, 3 steps are set up to collect users' requirements. Step 1 is asked for choosing a deployment model and the default choice is public cloud. There is a help button available beside step 1 question, which can activate a drop-down text field of hints, as shown in Figure 5.4. This aims to help the user for a better understanding of the definition of deployment models and making an appropriate determine.

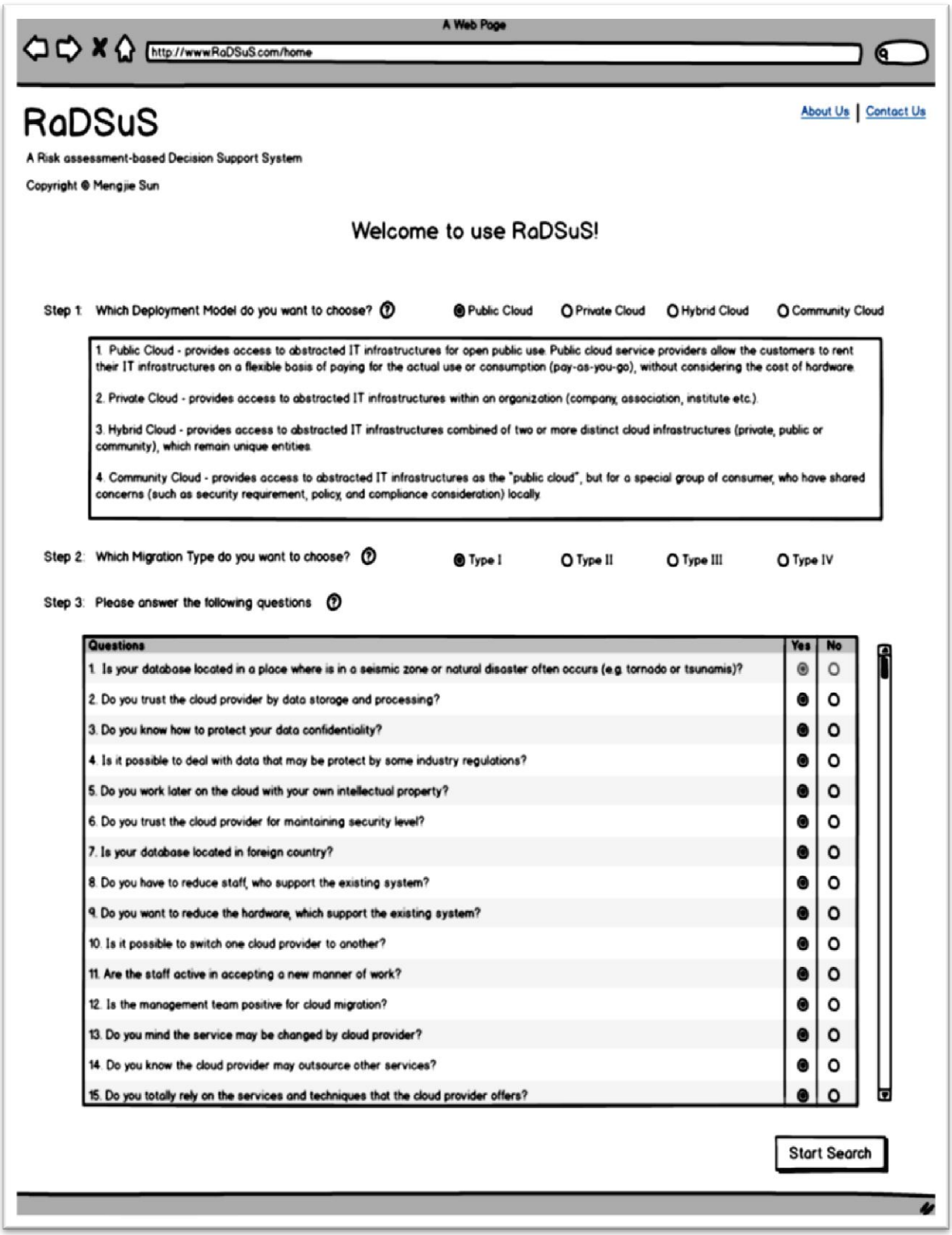

Figure 5.4: Hints of Deployment Models

Step 2 is about choosing the migration type. In the section, we have already explained how to classify the migration in four types. However, the concepts of migration type may be unfamiliar to the user and a corresponding hint is on demand, which is shown in Figure 5.5. The default setting of migration type is Type I.

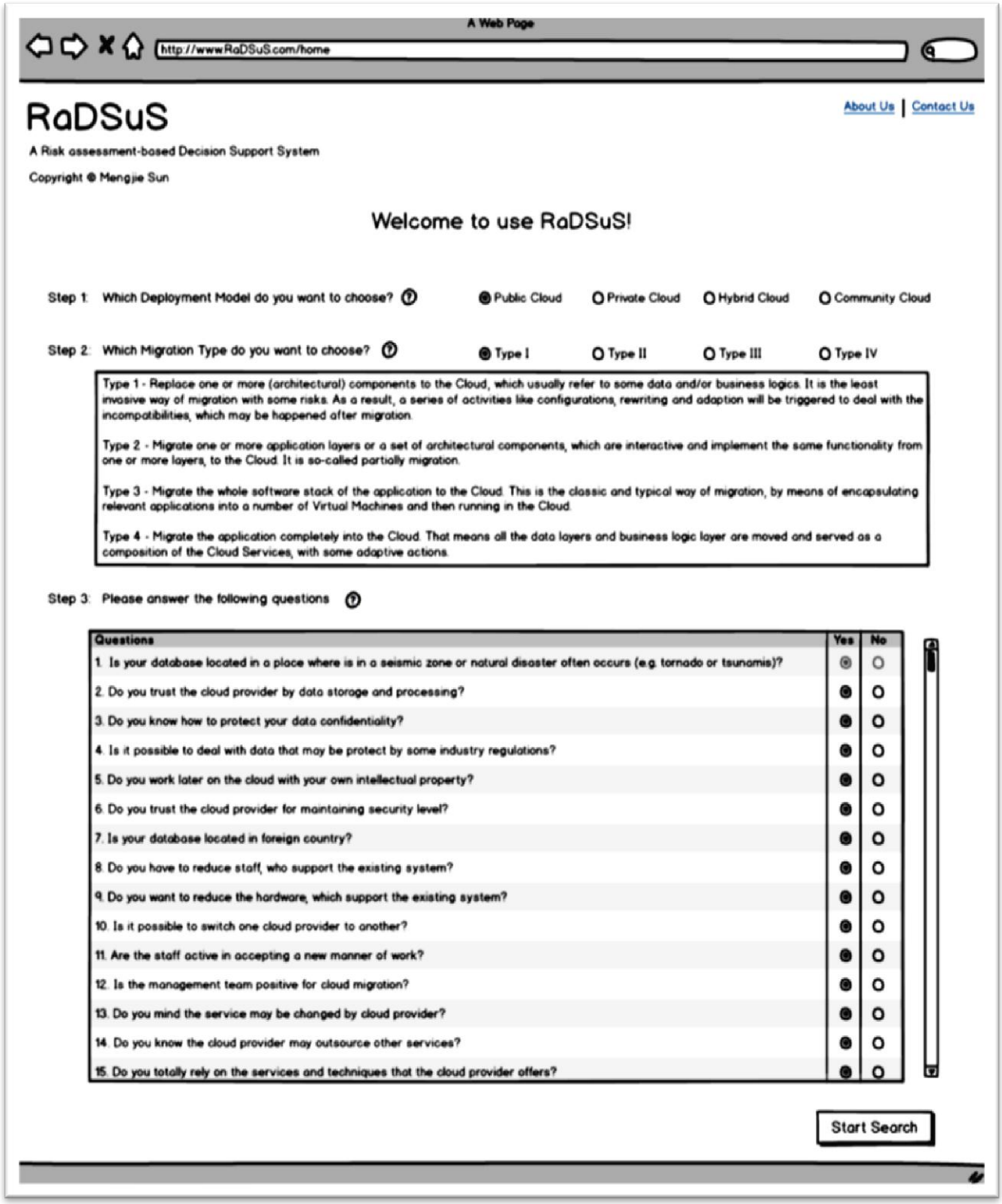

Figure 5.5: Hints of migration types

In step 3, a series of questions are asked for aiming to specify the requirements for a better searching ability of risks. These questions are for the IT experts and developers with concerning knowledge, as shown in Figure 5.6. There are also some explanations before answering these questions by clicking the button with question mark, about which are for those normal user who has no ideas. With a definite window of this UI, a scroll bar is needed here to maintain the concision of the interface. Each question will be answered with a ration box as same as the former two steps to keep the choice unique.

The default answer of each question is yes if the user leaves the question with no answer, the system will return all the possible risks.

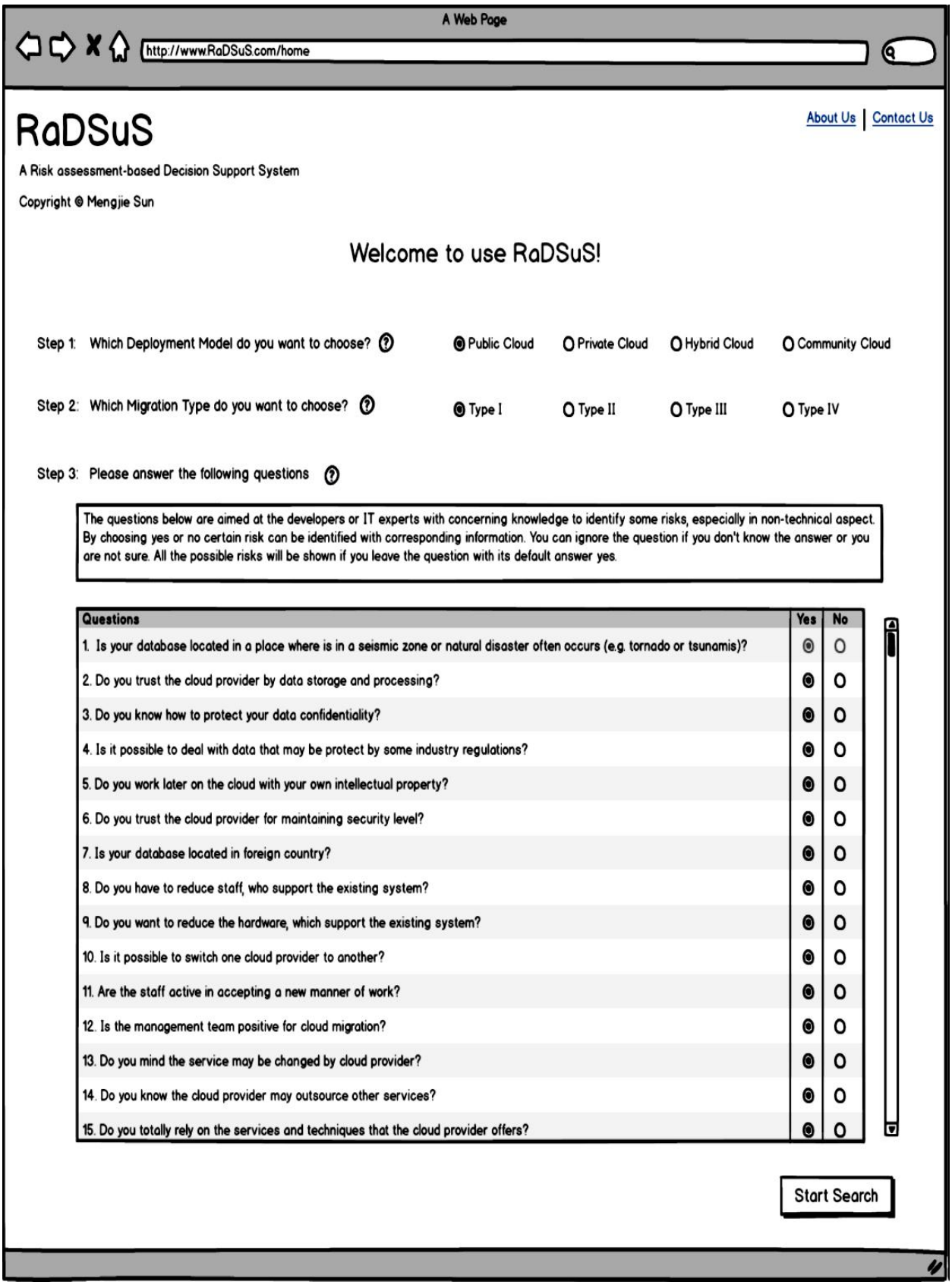

Figure 5.6: hints before answering the questions

There are some constraints applied here in step 3. When the user has chosen private cloud in step 1, some questions are fading out due to the constraints in the database. This facilitates the questionnaire step for avoiding the user to answer the question which is related to identifying those risks that has been already removed from the result in the first step. Figure 5.7 demonstrates exactly this scenario. The first question is your database located in a place where is in a seismic zone or natural disaster often occurs (e.g. tornado or tsunamis)?" is default to be disabled because the default setting in step 1 is public cloud and this corresponding risk is exclusive from the search field of public cloud. We believe that this risk rarely happens by public cloud because the public cloud provider usually has a set of mechanisms to avoid its occurrence or an alternate backup data center. This will be presented in the main page of the system shown in Figure 5.3.

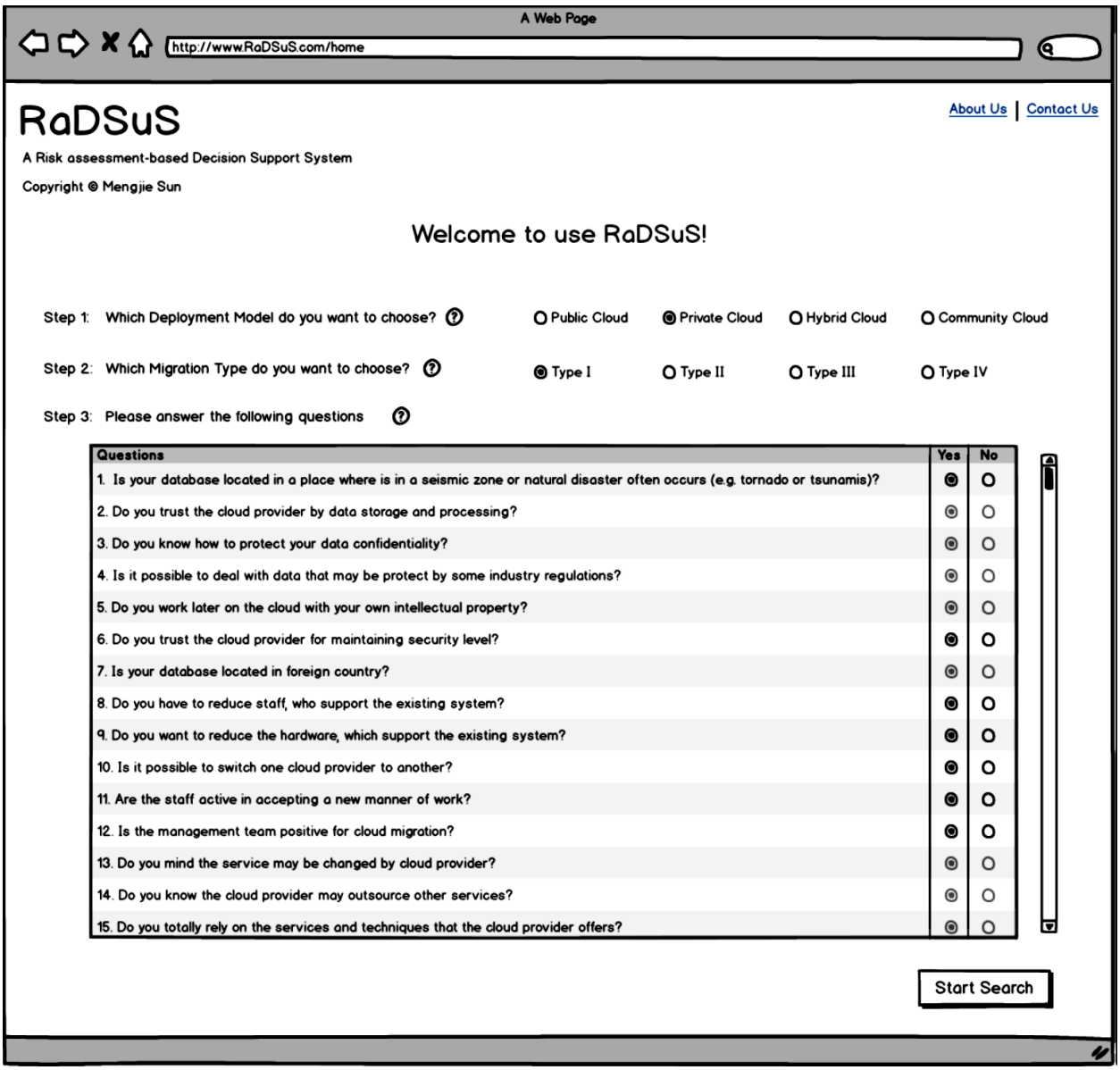

Figure 5.7: Questions when choosing private cloud and migration type I

When all 3 steps are finished, a search order will be submitted by clicking the Start Search button. Then the system will retrieve all the risks referring to the requirements and return a catalogue of risks with associated information. And the interface for displaying the results is activated, as shown in Figure 5.8. In this page the upper part is remained from the home page and the lower part is turned to a listing of result. The most important features of risks such as risk name, context of occurrence and risk mitigation methods are involved for presentation. In additional there is a button for a drop-down table of other attributes in the end of each risk column, as illustrated in Figure 5.9.

Since there are all kinds of information in our risk catalogue and these should be shown optionally to meet the users requires. As needed, the user can ask for a new search with changes of requirements by clicking the button New Search, which navigates users to go back to the home page of the system.

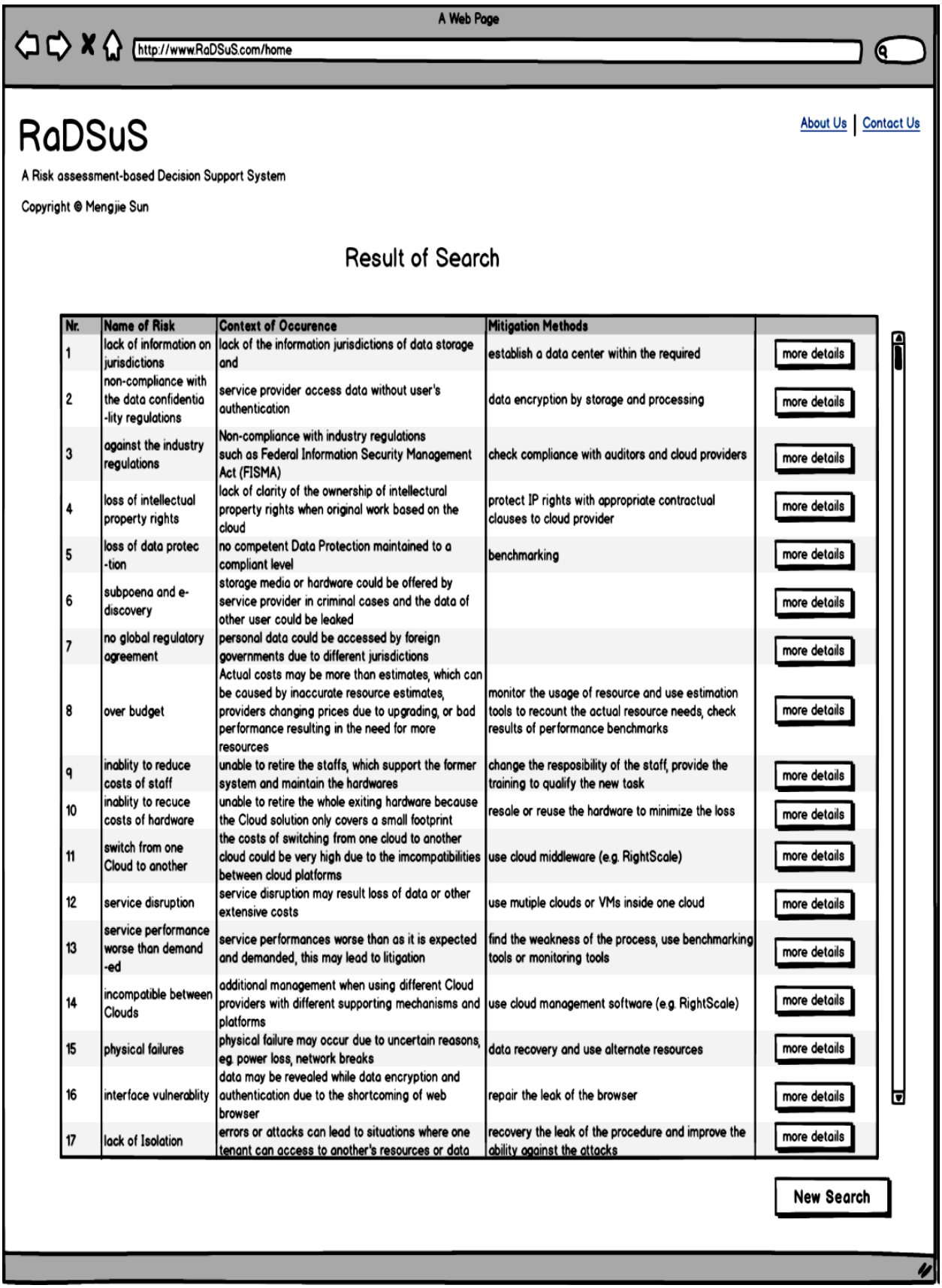

Figure 5.8: Result of the risk search

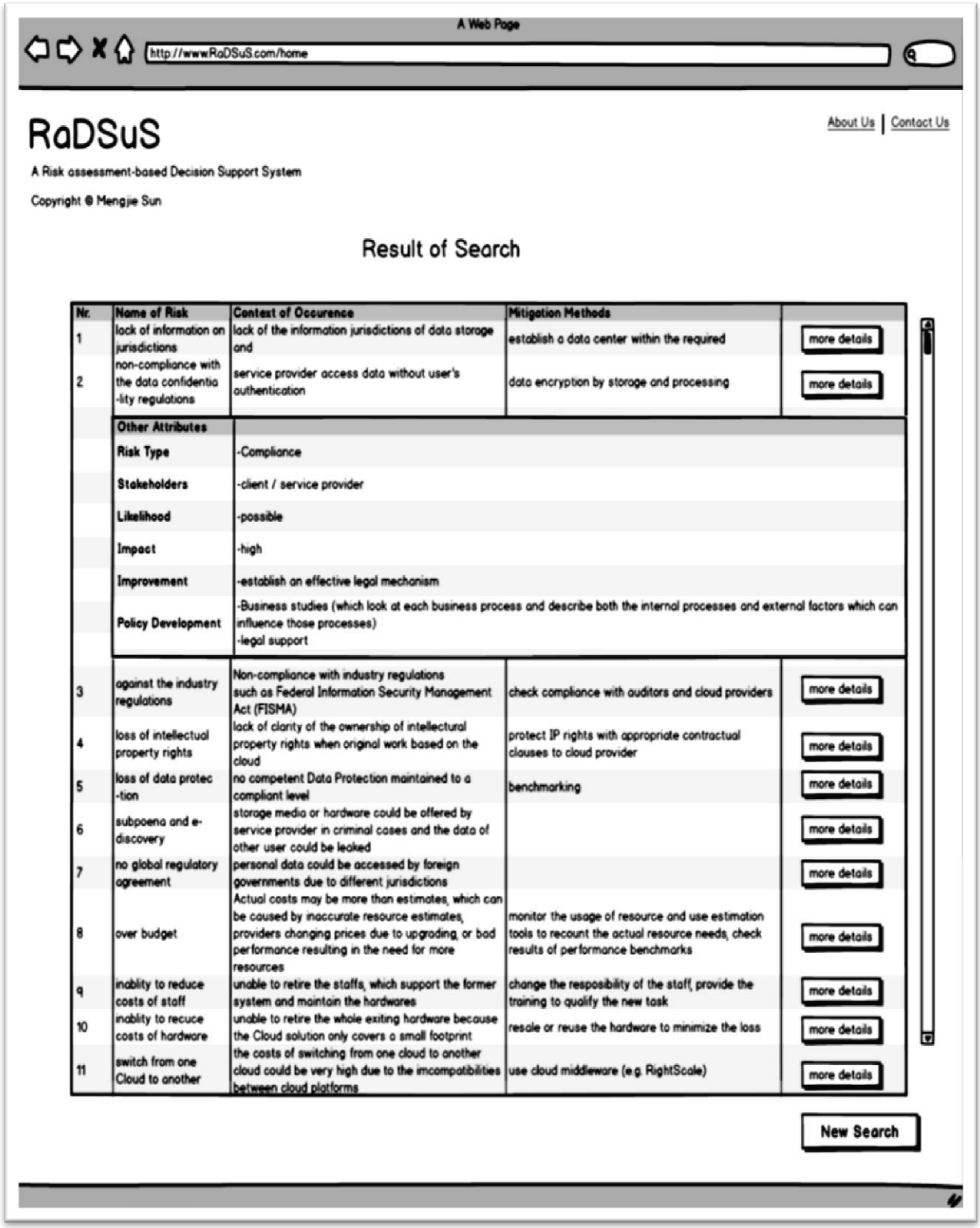

Figure 5.9: Other Attributes of the Risk

5.4 Implementation

This system is named RaDSuS that comes from the abbreviation of Risk assessment based Decision Support System. It is developed on the Windows and run on the Tomcat. For the database layer, Postgresql is chosen due to its advantages in free-for-use and programmability. This system will be written in Java on the IDE Eclipse Kepler JEE and represented in HTML, JSP, JS and CSS. A structured illustration is shown in Figure 5.10.

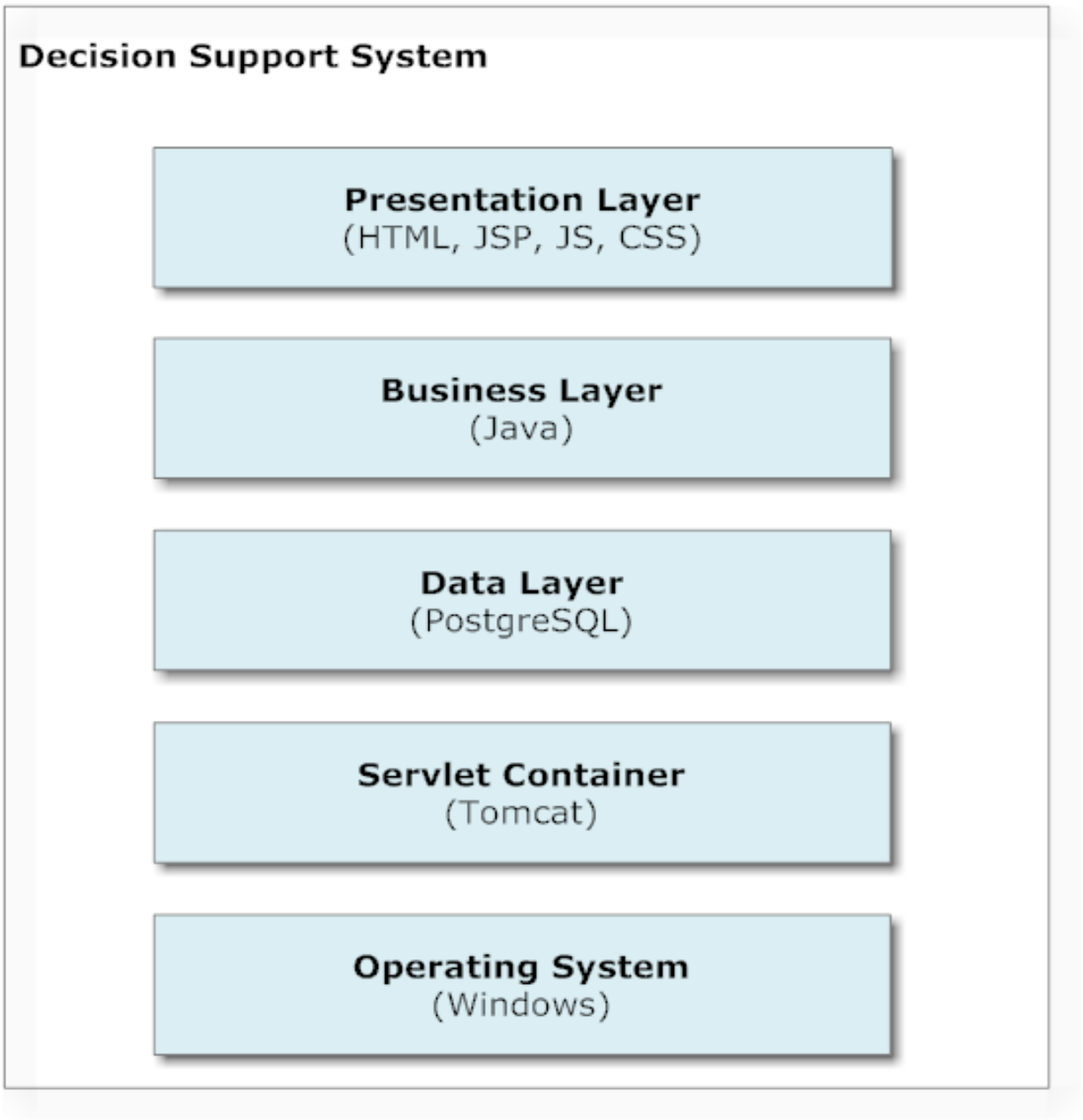

Figure 5.10: Layer model with implementaion

5.4.1 Risk database

In order to gain more scalability and save development and licensing costs, an open- source software solution is on demand for implementing database. PostgreSQL is an object-relational database management system with an emphasis on extensibility and standards compliance. The data queries can be easy realized by using SQL language as same as other common database systems, e.g. data are linked together with the Foreign Key. Moreover there are many high-quality GUI Tools available for PostgreSQL from both open source developers and commercial providers. Due to the stability as well as the programmability PostgreSQL is chosen for the database implementation of this system.

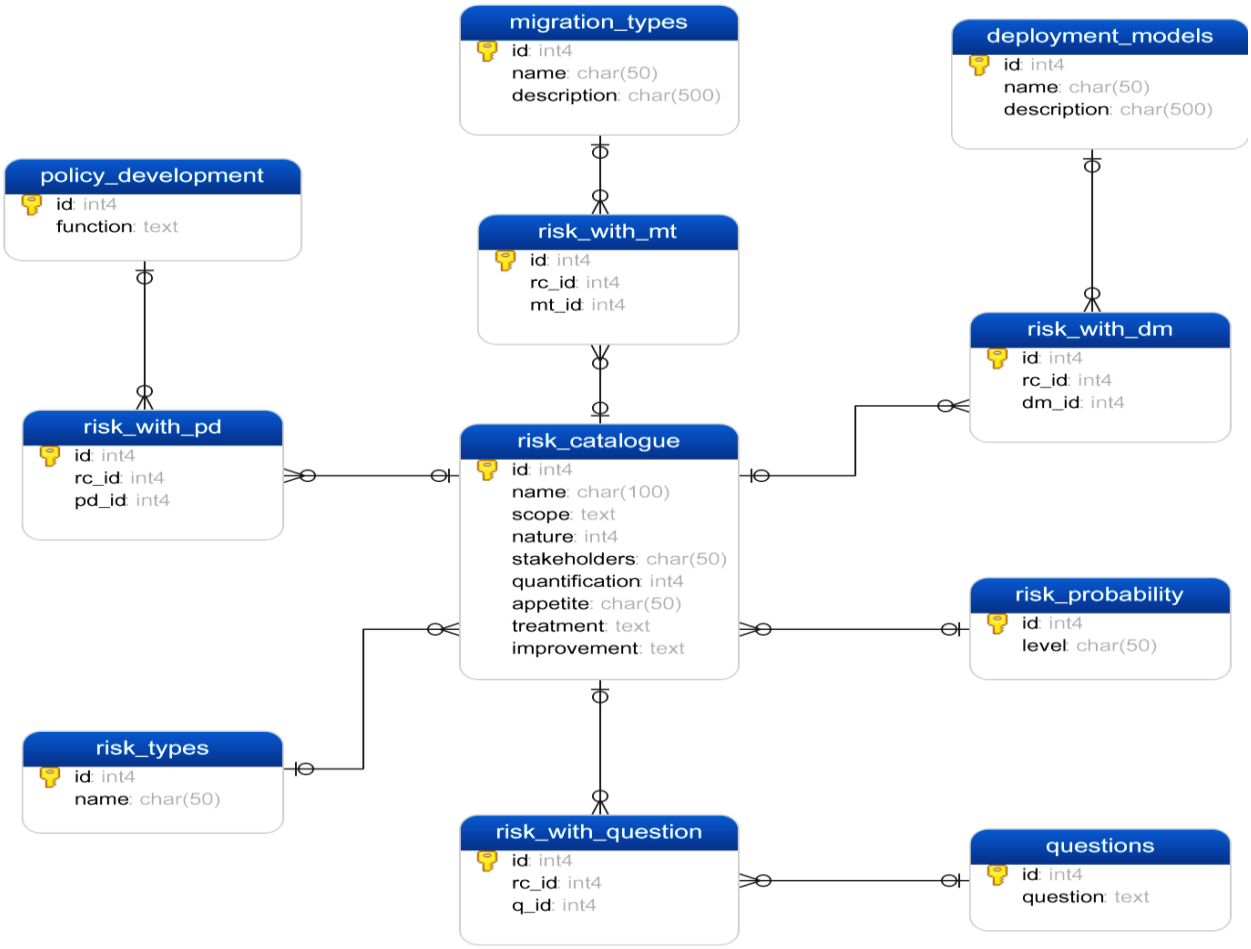

Figure 5.11: Data Model of Decision Support System

The risk database is implemented as a relational database on the basis of the corresponding ER model in Figure 5.2. And Figure 5.11 presents a data model of RaDSuS. This database consists of 11 entities. The entity risk catalogue acts as the basic element and all the other entities are

direct or indirect related to it. There are 4 deployments models and 46 risks. Each model is related to different number of risks, which build totally 161 combinations of relations between these two entities. Similarly, 4 migrations types build 77 combinations in all with 46 risks, since the migration type is supposed to be only related to those risks in Knowledge Management. Questions are used to identify other types of risks which have a one-to-many relationship with risk catalogue. Besides, the robability and types have both a one to much relationship with risk catalogue since each risk has only one risk type and one probability of occurrence. The id in risk probability and in risk type acts as foreign keys referencing to quantification and nature in risk catalogue.

5.5 Summary

In this section, a risk assessment-based decision support system named RaDSuS is revealed from concept to implementation phrase. In the meantime, the requirements as well as the specifications of this system are firstly discussed, which include some details in function, interaction, data and system independence. Then a conceptual framework is given which consists of a UI as frontend and a database as Backend. ER-diagram and UI mockups are used to explain the structure of database and HMI. This system is designed as a RESTful Web Service system with implementation in JEE and represention in HTML, JSP, JS and CSS. All the resources are identified by URIs and represented as XML and JSON, while PostgreSQL is chosen to build a rational database of this system.

CHAPTER SIX
CONCLUSION AND FUTURE RECOMMENDATIONS

6.1 Conclusion

With the expansion of IT techniques and the increasing amount of researches and reports, risk assessment is gradually realized as an essential tool for every medium and large scare organization. Because it help to identify the missing gap, that could interrupt the business continuity and down time of the organization and to be proactive and the help of cloud computing, and disaster recovery plans pose a both an opportunity and a challenge for enterprises. It benefits the cloud users by opening an efficient on-demand service and enables enterprises to pay more attentions to developing business instead of investment, setup and maintain their own hardware. With the advantages in scalability, high-level availability, edibility and easy-using cloud computing is now evolving like never before, with enterprises of all types and scales adapting to this new technology. However, the security issues should be undoubtedly considered since many use cases evidence that there are certain issues and problems accompanied with those advantages. It is very helpful to recognize the risks associated as much as possible before determining migrating to the cloud. Therefore, a comprehensive understanding of risks that may be treaty with is quite important for a rational decision. Furthermore, an easy using decision support system based on risk assessment is also proposed in this work.

To achieve these goals, some related works have been identified, which involves the basic knowledge of cloud computing and decision support system for cloud migration. Then we have discussed the risk management issues and learned the standards of risk definition by IRM, which is as the basis of our new catalogue of risks that may occur by applications adoption to the cloud. In order to simplify the recognition of all risks, a decision support system as an intuitive method has been proposed instead of traditional workshop or arrangement meeting. This user-friendly system named RaDSuS is targeted on showing all the possible risks that the user might confront, with satisfying the users requirements by choosing deployment model and migration type as well as answering some specific questions. This system is designed as a Restful Web service, by which all the resources are identified by URIs and represented as XML and JSON data format.

The user interface of this system acts as frontend which is built on JSP with Servlet, while a rational risk database structured in PostgreSQL as backend RaDSuS are proved to be able to specify the users requirements and give the decision maker a general understanding of all risk sassociated by cloud migration.

6.2 Future Recommendations

In this research various risks has been tendered with the IRM standard of risk description and successfully applied it into a new decision support system for risk assessment, there are still some limitations of the catalogue as well as the system themselves and some improvement are require for the future work.

It is strongly advised to subdivide this category Knowledge Management into such as knowledge concerning and technique implemental, in order to get a better understanding of when and where the risks may occur and how best medium and large scale organization can mitigate and prepared for any kind risk and disasters. Organizations must keep in touch with the cloud services providers in order to ensure their data are secure, up to date and available when needed.

This catalogue summarizes all the risks according to large amount of references and case studies and identifies risk in a general art of definition, i.e. some risks are generalized as one risk. So it is relative difficult to address the risks to the migrating components, by which we implement in our system with some exact questions. It could be accomplished in a proceeding work of research. The decision support system aims to return all the possible risks with detailed information for a general understanding according to the requirement of this thesis, but with no needs to score and rank of risks. There are lots of researches on how to assess and evaluate the risks with weights and in this work we have also identified the likelihood and impact with some scores. With these factors we could list all the risks with some specific requirements such as displaying top 10 risks with largest impacts or listing top 5 risks in particular risk type in the future work.

Although we have reddened all the risks with the IRM standard of risk description and successfully applied it into a new decision support system for risk assessment, there are still some limitations of the catalogue as well as the system themselves and some improvement can be also recommended in the future work. The risk catalogue classifies all the 46 risks in 5 categories. However the risks in type Knowledge Management are in the majority comparing to other types of risks, e.g. there are only 5 risks in Strategic and 4 in Financial. It is strongly advised to subdivide this category Knowledge Management into such as knowledge concerning

and technique implemental, in order to get a better understanding of when and where the risks may occur.

This catalogue summarizes all the risks according to large amount of references and case studies and identifies risk in a general art of definition, i.e. some risks are generalized as one risk. So it is relative difficult to address the risks to the migrating components, by which we implement in our system with some specific questions. It could be accomplished in a proceeding work of research. The decision support system aims to return all the possible risks with detailed information for a general understanding according to the requirement of this thesis, but with no needs to score and rank of risks. There are lots of researches on how to assess and evaluate the risks with weights and in this work we have also identified the likelihood and impact with some scores. With these factors we could list all the risks with some specific requirements such as displaying top 10 risks with largest impacts or listing top 5 risks in particular risk type in the future work.

REFERENCES

Alhazmi, O. H. (2015). Computer-aided disaster recovery planning tools (CADRP). *International Journal of Computer Science & Security (IJCSS)*, *9*(3), 132-139.

Andrikopoulos, V., Strauch, S., & Leymann, F. (2013). Decision Support for Application Migration to the Cloud-Challenges and Vision. In *CLOSER* (pp. 149-155).

Athukorala, P. C., & Resosudarmo, B. P. (2005). The Indian Ocean tsunami: Economic impact, disaster management, and lessons. *Asian Economic Papers*, *4*(1), 1-39.

B. Priyadharshini, B., & Parvathi, P. (2012, March). Data integrity in cloud storage. In *Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on* (pp. 261-265). IEEE.

Chapman, C., & Ward, S. (2003). *Project risk management: processes, techniques, and insights*. Wiley.

Day, J. M., Melnyk, S. A., Larson, P. D., Davis, E. W., & Whybark, D. C. (2012). Humanitarian and disaster relief supply chains: a matter of life and death. *Journal of Supply Chain Management*, *48*(2), 21-36.

E. Network and I. S. Agency, \Cloud computing: benefits, risks and recommendations for information security," tech. rep.,. (2012, December).

Elastic Compute Cloud (EC2) – Cloud Server & Hosting – AWS. (n.d.). Retrieved June 13, 2017, from http://aws.amazon.com/ec2

Eureka moments brought to you by analytics on IBM Cloud. (2016, February 19). Retrieved June 13, 2017, from http://www.ibm.com/cloudcomputing/us/en/iaas.html

Fitó, J. O., & Guitart, J. (2014). Business-driven management of infrastructure-level risks in Cloud providers. *Future Generation computer systems*, *32*, 41-53.

Getter, J. R. (2007, January). Enterprise architecture and IT governance: A risk-based approach. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on* (pp. 220-220). IEEE.

H., S. , H., H, A., M., & T, K. (2014.). Risk factors in software development phases.

Khdour, T., & Hijazi, H. (2012). A step towards preventive risk management in software projects. In *International Conference on Software Technology and Engineering (ICSTE 2012)*. ASME Press.

Kote, A., Raja, P. V. K., & Raju, M. V. (2015). Cloud Data Security Challenges and its Solutions. *IJCCER*, *3*(5), 89-92.

Legacy, M. P. F. (2015). A Quantitative Study On Migration Path From Legacy System To Contemporary Systems.

Loayza, N. V., Olaberria, E., Rigolini, J., & Christiaensen, L. (2012) & PUNDIT CAFÉ (2016). Natural disasters and growth: going beyond the averages. *World Development*, *40*(7), 1317-1336.

Lyons, B. (2006). Preparing for a disaster: Determining the essential functions that should be up first. *SANS Institute*.

Manaktala, R. S. (2013). *Optimization of Disaster Recovery Leveraging Enterprise Architecture Ontology* (Doctoral dissertation, The Ohio State University).

Mohamed Shaluf, I. (2007). An overview on disasters. *Disaster Prevention and Management: An International Journal*, *16*(5), 687-703.

NIST, S. P. (1995). 800-12: An Introduction to Computer Security–The NIST Handbook.

Peacock, W. G., Dash, N., & Zhang, Y. (2007). Sheltering and housing recovery following disaster. *Handbook of disaster research*, 258-274.

Rapp, R. R. (2011). *Disaster recovery project management: Bringing order from chaos*. Purdue University Press.

Rudawitz, D. (2003, November). Enterprise Architecture and Disaster Recovery Planning. Enterprise IT Solutions LLC,

Samad, J., Loke, S. W., & Reed, K. (2013, July). Quantitative Risk Analysis for Mobile Cloud Computing: A Preliminary Approach and a Health Application Case Study. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on* (pp. 1378-1385). IEEE.

Schneider, S. K. (2005). Administrative breakdowns in the governmental response to Hurricane Katrina. *Public Administration Review*, *65*(5), 515-516

Schulman, R. R. (2004). Disaster recovery issues and solutions. *A White Paper, Hitachi Data Systems*.

Shahzad, B., & Safvi, S. A. (2008). Effective risk mitigation: a user prospective. *International Journal of Mathematics and Computers in Simulation*, *2*(1), 70-80.

Staff, S. (2012, June 14). 5 Tips to Build an Effective Disaster Recovery Plan. Retrieved June 13, 2017, from http://www.smallbusinesscomputing.com/News/ITManagement/5-tips-to-build-an-effective-disaster-recovery-plan.html

Sun, M. (2014). *Risk assessment-based decision support for the migration of application to the cloud* (Master's thesis).

Swanson, M. (2001). NIST Special Publication 800-26 Security Self-Assessment Guide for Information Technology Systems. *National Institute of Standards and Technology*.

Swanson, M. (2001). *Security self-assessment guide for information technology systems* (No. NIST-SP-800-26). BOOZ-ALLEN AND HAMILTON INC MCLEAN VA.

Types of Natural Disasters: Features & Examples. (2017, March 30). Retrieved June 13, 2017, from http://www.punditcafe.com/science/types-of-natural-disasters-examples/

Viduto, V., Maple, C., Huang, W., & López-Peréz, D. (2012). A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem. *Decision Support Systems*, *53*(3), 599-610.

Curtis Preston, “Data Protection Strategies In Today’s Data Center”, Oracle whitepaper, January 2012.

Whybark, D. C. (2007). Issues in managing disaster relief inventories. *International Journal of Production Economics*, *108*(1), 228-235.\

Whybark, D. Clay. "Issues in managing disaster relief inventories." *International Journal of Production Economics* 108, no. 1 (2007): 228-235.

Wright, C. S. (2012). A Preamble into Aligning Systems Engineering and Information Security Risk Measures. In *International Conference on Electronics, Information and Communication Engineering (EICE 2012)*. ASME Press.

Wu, Z. Y., & Khaliefa, M. (2012). Cloud computing for high performance optimization of water distribution systems. In *World Environmental and Water Resources Congress 2012: Crossing Boundaries* (pp. 679-686).

Yi, W., & Kumar, A. (2007). Ant colony optimization for disaster relief operations. *Transportation Research Part E: Logistics and Transportation Review*, *43*(6), 660-672.

Younge, A. J., Henschel, R., Brown, J. T., Von Laszewski, G., Qiu, J., & Fox, G. C. (2011, July). Analysis of virtualization technologies for high performance computing environments. In *Cloud Computing (CLOUD), 2011 IEEE International Conference on* (pp. 9-16). IEEE.

APPENDICES

APPENDIX 1
DATA

I. Consider two Apps A and B having RTA 10hrs and 15hrs respectively; both would be recovered in 15hrs, but if A is prioritized, then recovery tasks that can be time-sliced, such as DNS changes, could mean A is recovered faster and no longer has a dollar loss associated with it. Time slicing is done for recovery of those Tech Components that are App specific and are not restored for the entire Enterprise at the same time. For example, DNS changes can be implemented for each App separately, but the Mainframe must be "up" as a whole and cannot be time-sliced.

II. Similarly, consider a C1 critical App A with RTA of 30hrs, dependent (say 4th or 5th level dependency) on an App B that has an RTO objective
41 of 48hrs (RTA may be further off); ordinarily, App 'B' would not be recovered out of turn as part of a Business Process, but it would be promoted in the recovery sequence as part of A's App Suite per RSA recovery.
RPO due to currency of backup is an assumed risk even though this metric does not govern dollar loss for downtime. An App is not 'up until all relevant data is synced and verified, and this can happen only after all the supporting Infrastructure is up. At Time of Disaster, the Data Sync would be a dynamic component and since RPA (Recovery Point Actual) is not predictable, RPO is not considered a Decision Support Metric for RSA recovery.

Recovering an App Suite versus an entire Business Process increases cost of recovering non-critical Apps supporting critical functionality. An App having lower criticality might be also supporting an App that's part of a Most Critical Business Process (MCBP), and would hence require additional budgeting for meeting a higher threshold of recovery capability, expected of an App being recovered as part of an App Suite supporting a MCBP. If Business Process did recovery, App dependencies across Business Processes would not get resolved until the entire supporting less-critical Business Process is recovered, which implies huge losses by downtime.

APENDIX 2
SOURCE CODE

A.AD[] -> List of apps that support A

A.Infra[] -> List of Infrastructure components that support A

A.AppRTA -> RTA for A including all apps that support A

A.Tech[].value -> Technology component checklist that support A

A.Tech[].start -> Start time for Recovery per ATOD assessment

A.Tech[].RTA -> RTA duration per ATOD assessment

A.Tech[].ASC -> App Suite Count recovered thus far

functioninitAppRTA(App A)

initTechList(A);

A.AppRTA=TechRTA(A); **for each** i**in**A.AD[]

A.AppRTA= max(A.AppRTA, initAppRTA(A.AD[i])) *// Stop further recursion if cycle detected*

returnA.AppRTA // If *A has no Apps that support it, AppRTA=TechRTA*

functioninitTechList(App A) *// Initialize Tech dependencies considering immediate child nodes*

for each i**in**A.AD

for each j **in** A.AD[i].Tech[]

if(A.AD[i].Tech[j].value==true**)**A.Tech[j].value=true; *//Propagate Tech dependencies* upwards

returnA.Tech[];

functionTechRTA(App A)

for each i**in**A.Tech[]

A.AppRTA=max(A.AppRTA, A.Tech[i].Start + min(1, A.Tech[i].RTA/Tech[i].ASC))

returnA.AppRTA

functionRSARecovery (App A[], Criticality)

for each i**in**A

If(A[i].Criticality==Criticality**)**

Add element A[i] **to** subsetA[]

L1 □□for each i**in**subsetA

initAppRTA(subsetA[i])

Sort subsetA**by**AppRTA

for each i**in**subsetA

Recover subsetA[i]

SubsetA[i].Tech [].value=false *//Tech checklist is reset to reflect recovered state*

SubsetA[i].Tech [].ASC++ *//Increment App Suite Counter for each associated Tech Component*

gotoL1 *// Update all AppRTAs to benefit from dependencies recovered*

RSARecovery (A, Criticality+1).

Tech Components are recovered in parallel and this optimization is achieved using ATOD start times and duration. If Tech Components have overlapping times on the recovery timeline, parallel recovery is implied and hence not explicitly dealt with in the algorithm, but instead expected as input from ATOD analysis.

Recovering components for a given App Suite has a dynamic impact on the RTA of Apps supported by it. As Components are recovered, dependencies are eliminated and what would have been the App with least time remaining to recover at a previous time step, might not be the case at the next time step. It is hence important to dynamically update the dependencies that still need to be recovered.